Audit Report

Metasploitable 2 - Full Audit

Audited on August 20 2012

Reported on August 21 2012

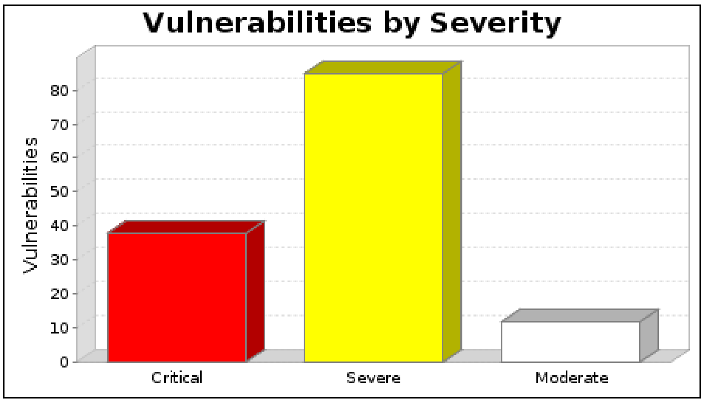
1. Executive Summary

This report represents a security audit performed by Nexpose from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

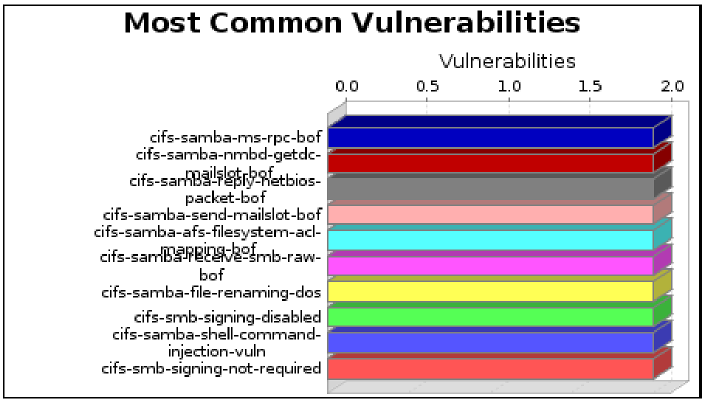
Site Name	Start Time	End Time	Total Time	Status
metasploitable2	August 20, 2012 16:04, EST	August 20, 2012 16:11, EST	6 minutes	Success

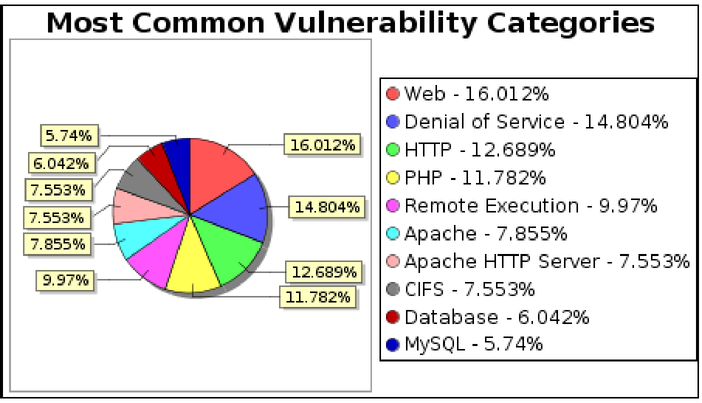
There is not enough historical data to display overall asset trend.

The audit was performed on one system which was found to be active and was scanned.

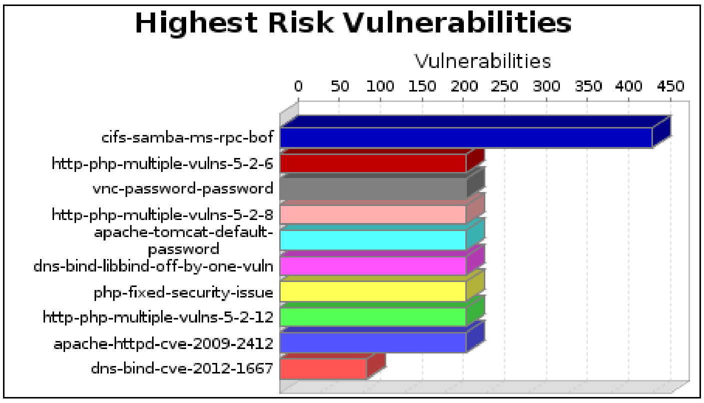


There were 135 vulnerabilities found during this scan. Of these, 38 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 85 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 12 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities.





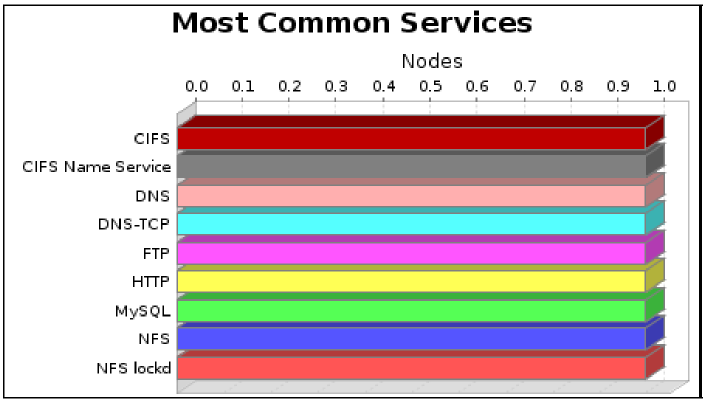
There were 2 occurrences of the cifs-samba-ms-rpc-bof, cifs-samba-nmbd-getdc-mailslot-bof, cifs-samba-reply-netbios-packet-bof, cifs-samba-send-mailslot-bof, cifs-samba-afs-filesystem-acl-mapping-bof, cifs-samba-receive-smb-raw-bof, cifs-samba-file-renaming-dos, cifs-smb-signing-disabled, cifs-samba-shell-command-injection-vuln and cifs-smb-signing-not-required vulnerabilities, making them the most common vulnerabilities. There were 53 vulnerabilities in the Web category, making it the most common vulnerability category.

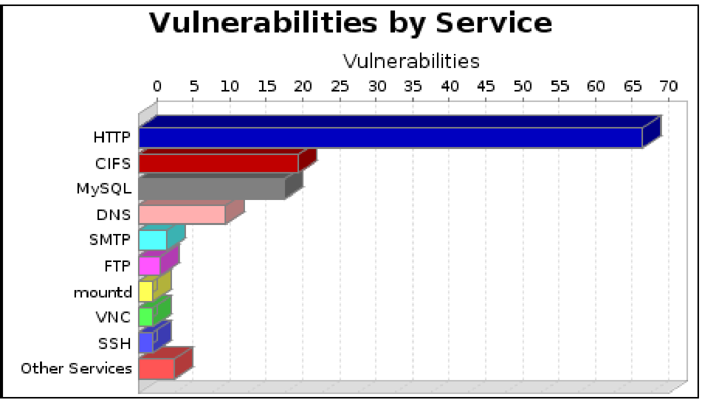


The cifs-samba-ms-rpc-bof vulnerability poses the highest risk to the organization with a risk score of 450. Vulnerability risk scores are calculated by looking at the likelihood of attack and impact, based upon CVSS metrics. The impact and likelihood are then multiplied by the number of instances of the vulnerability to come up with the final risk score.

One operating system was identified during this scan.

There were 22 services found to be running during this scan.





The CIFS, CIFS Name Service, DNS, DNS-TCP, FTP, HTTP, MySQL, NFS and NFS lockd services were found on 1 systems, making them the most common services. The HTTP service was found to have the most vulnerabilities during this scan with 69 vulnerabilities.

2. Discovered Systems

Node	Operating System	Risk	Aliases
192.168.56.3	Ubuntu Linux 8.04	55,660	•METASPLOITABLE •metasploitable.localdomain

3. Discovered and Potential Vulnerabilities

3.1. Critical Vulnerabilities

3.1.1. Apache HTTPD: APR apr_palloc heap overflow (CVE-2009-2412) (apache-httpd-cve-2009-2412)

Description:

The affected asset is vulnerable to this vulnerability ONLY if a non-Apache application can be passed unsanitized user-provided sizes to the apr_palloc() function. Review your Web server configuration for validation.The affected asset is vulnerable to this vulnerability ONLY if a non-Apache application can be passed unsanitized user-provided sizes to the apr_palloc() function. Review your Web server configuration for validation.A flaw in apr_palloc() in the bundled copy of APR could cause heap overflows in programs that try to apr_palloc() a user controlled size. The Apache HTTP Server itself does not pass unsanitized user-provided sizes to this function, so it could only be triggered through some other application which uses apr_palloc() in a vulnerable way.

Affected Nodes:

Affected Nodes:	**Additional Information:**
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	**Reference**
APPLE	APPLE-SA-2009-11-09-1
BID	35949
CVE	CVE-2009-2412
OSVDB	56765
OSVDB	56766
OVAL	OVAL8394
OVAL	OVAL9958
SECUNIA	36138
SECUNIA	36140
SECUNIA	36166
SECUNIA	36233
SECUNIA	37152
SECUNIA	37221
SUSE	SUSE-SA:2009:050
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache >= 2.2 and < 2.2.13

Upgrade to Apache HTTPD version 2.2.13

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.13.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.1.2. Tomcat Application Manager Tomcat Tomcat Password Vulnerability (apache-tomcat-default-password)

Description:

The Tomcat service administrator user 'tomcat' has a password which is set to a value 'tomcat'. As a result, anyone with access to the Tomcat port can trivially gain full access to the machine.

Affected Nodes:

Affected Nodes:	**Additional Information:**

192.168.56.3:8180	Running vulnerable HTTP service: Apache Tomcat.
	Based on the following 2 results:http://192.168.56.3:8180/manager/html
	
	http://192.168.56.3:8180/manager/html
	`82:     <img border="0" alt="The Apache Software Foundation" align="left"`
	`83:          src="/manager/images/asf-logo.gif">`
	`84:    </a>`
	`85:    <a href="http://tomcat.apache.org/">`
	`82: ...="0" alt="The Tomcat Servlet/JSP Container"`

References:

Source	**Reference**
BID	38084
CVE	CVE-2009-3843
CVE	CVE-2010-0557
OSVDB	60317
OSVDB	62118

Source	Reference
SECUNIA	37444
SECUNIA	38457
XF	operations-manager-unspecified-sec-bypass(54361)

Vulnerability Solution:

The Tomcat service has an administrator account set to a default configuration. This can be easily changed in conf/tomcat-users.xml

3.1.3. Samba NDR Parsing Heap Overflow Vulnerability (cifs-samba-ms-rpc-bof)

Description:

Samba's NDR parsing code is vulnerable to multiple heap overflows via crafted MS-RPC requests such as "DFSEnum," "RFNPCNEX," "LsarAddPrivilegesToAccount," "NetSetFileSecurity," and "LsarLookupSids/LsarLookupSids2." Successful exploitation allows an unauthenticated attacker to execute arbitrary commands as root.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:139	Running vulnerable CIFS service: Samba 3.0.20-Debian.
192.168.56.3:445	Running vulnerable CIFS service: Samba 3.0.20-Debian.

References:

Source	Reference
APPLE	APPLE-SA-2007-07-31
BID	23973
BID	24195
BID	24196
BID	24197
BID	24198
BID	25159
CERT-VN	773720
CVE	CVE-2007-2446
DEBIAN	DSA-1291
OSVDB	34732
OVAL	OVAL11415
REDHAT	RHSA-2007:0354
SECUNIA	25232
SECUNIA	25241
SECUNIA	25246

Source	Reference
SECUNIA	25251
SECUNIA	25255
SECUNIA	25256
SECUNIA	25257
SECUNIA	25259
SECUNIA	25270
SECUNIA	25289
SECUNIA	25567
SECUNIA	25675
SECUNIA	25772
SECUNIA	26235
SECUNIA	26909
SECUNIA	27706
SECUNIA	28292
SUSE	SUSE-SA:2007:031
URL	http://samba.org/samba/security/CVE-2007-2446.html
XF	samba-lsaioprivilegeset-bo(34309)
XF	samba-lsaiotransnames-bo(34316)
XF	samba-netdfsiodfsenuminfod-bo(34311)
XF	samba-secioacl-bo(34314)
XF	samba-smbionotifyoptiontypedata-bo(34312)

Vulnerability Solution:

Download and apply the upgrade from: http://us1.samba.org/samba/ftp/old-versions/samba-3.0.25.tar.gz

3.1.4. BIND libbind inet_network() Off By One Vulnerability (dns-bind-libbind-off-by-one-vuln)

Description:

An off-by-one error in the inet_network function in libbind could allow context-dependent attackers to cause a denial of service and possibly execute arbitrary code via specially crafted input that triggers memory corruption.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:53	Running vulnerable DNS service: BIND 9.4.2.

References:

Source	Reference

Source	Reference
BID	27283
CERT-VN	203611
CVE	CVE-2008-0122
OVAL	OVAL10190
REDHAT	RHSA-2008:0300
SECUNIA	28367
SECUNIA	28429
SECUNIA	28487
SECUNIA	28579
SECUNIA	29161
SECUNIA	29323
SECUNIA	30313
SECUNIA	30538
SECUNIA	30718
XF	freebsd-inetnetwork-bo(39670)

Vulnerability Solution:

•Upgrade to BIND version 9.3.5

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.3.5/bind-9.3.5.tar.gz
Upgrade to 9.3.5 version of ISC BIND Which was released on April 14, 2008. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.4.3

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.4.3/bind-9.4.3.tar.gz
Upgrade to 9.4.3 version of ISC BIND Which was released on November 19, 2008. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.5.0

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.5.0/bind-9.5.0.tar.gz
Upgrade to 9.5.0 version of ISC BIND Which was released on May 29, 2008. The source code and binaries for this release can be downloaded from bind's website.

3.1.5. PHP Multiple Vulnerabilities Fixed in version 5.2.12 (http-php-multiple-vulns-5-2-12)

Description:

Fixed a safe_mode bypass in tempnam() identified by Grzegorz Stachowiak (CVE-2009-3557)

Fixed a open_basedir bypass in posix_mkfifo() identified by Grzegorz Stachowiak (CVE-2009-3558)

Added "max_file_uploads" INI directive, which can be set to limit the number of file uploads per-request to 20 by default, to prevent possible DOS via temporary file exhaustion (CVE-2009-4017)

Added protection for $_SESSION from interrupt corruption and improved "session.save_path" check, identified by Stefan Esser (CVE-2009-4143)

Fixed bug #49785 (insufficient input string validation of htmlspecialchars()) (CVE-2009-4142)

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2010-03-29-1
BID	37389
BID	37390
CVE	CVE-2009-3557
CVE	CVE-2009-3558
CVE	CVE-2009-4017
CVE	CVE-2009-4142
CVE	CVE-2009-4143
DEBIAN	DSA-1940
DEBIAN	DSA-2001
OVAL	OVAL10005
OVAL	OVAL10483
OVAL	OVAL6667
OVAL	OVAL7085
OVAL	OVAL7396
OVAL	OVAL7439
SECUNIA	37412
SECUNIA	37482
SECUNIA	37821
SECUNIA	38648
SECUNIA	40262
SECUNIA	41480
SECUNIA	41490
URL	http://www.php.net/ChangeLog-5.php#5.2.12
URL	http://www.php.net/releases/5_2_12.php

Source	Reference
XF	php-multipart-formdata-dos(54455)

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.2.12.tar.gz/from/a/mirror
Upgrade to PHP v5.2.12 (released on December 17th, 2009).

3.1.6. PHP Multiple Vulnerabilities Fixed in version 5.2.6 (http-php-multiple-vulns-5-2-6)

Description:

Certain versions of PHP ship with flawed implementations of the init_reauest_info() and escapeshellcmd() functions, the GENERATE_SEED macro, and FastCGI SAPI.

The init_request_info() function does not properly calculate the length of PATH_TRANSLATED due to improper operator precedence handling. This could allow a remote attacker to execute arbitrary code via a crafted URI (CVE-2008-0599).

The FastCGI SAPI contains a stack-based overflow of unknown impact and attack vector (CVE-2008-2050).

The escapeshellcmd API function is vulnerable to an attack of unknown impact via a context-dependent attack (CVE-2008-2051).

The GENERATE_SEED macro can produce a zero seed. This could allow a remote attacker to bypass protection mechanisms via subsequent values based on the initial seed (CVE-2008-2107, CVE-2008-2108).

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2008-07-31
BID	29009
CVE	CVE-2008-2050
CVE	CVE-2008-2051
CVE	CVE-2008-2107
CVE	CVE-2008-2108
DEBIAN	DSA-1572
DEBIAN	DSA-1578
DEBIAN	DSA-1789
OVAL	OVAL10256
OVAL	OVAL10644
OVAL	OVAL10844
REDHAT	RHSA-2008:0505

Source	Reference
REDHAT	RHSA-2008:0544
REDHAT	RHSA-2008:0545
REDHAT	RHSA-2008:0546
REDHAT	RHSA-2008:0582
SECUNIA	30048
SECUNIA	30083
SECUNIA	30158
SECUNIA	30288
SECUNIA	30345
SECUNIA	30411
SECUNIA	30757
SECUNIA	30828
SECUNIA	30967
SECUNIA	31119
SECUNIA	31124
SECUNIA	31200
SECUNIA	31326
SECUNIA	35003
XF	php-fastcgisapi-bo(42133)
XF	php-generateseed-security-bypass(42284)
XF	php-generateseed-weak-security(42226)

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.6.tar.gz
Upgrade to PHP v5.2.6.

3.1.7. PHP Multiple Vulnerabilities Fixed in version 5.2.8 (http-php-multiple-vulns-5-2-8)

Description:

Certain versions of PHP ship with a vulnerable version of the PCRE library. This could allow a context-dependent attacker to cause a denial of service (crash) via a specially crafted regular expression. (CVE-2008-2371)

The imageloadfont() function could allow a context-dependent attacker to cause a denial of service (crash) via a crafted font file. (CVE-2008-3658)

The memnstr() function could allow a context-dependent attacker to cause a denial of service (crash) via the delimiter argument to the explode function. (CVE-2008-3659)

Certain versions of PHP, when used as a FastCGI module, could allow a remote attacker to cause a denial of service (crash). (CVE-2008-3660)

Certain versions of PHP ship with a heap-based buffer overflow in the mbstring extension. This could allow context-dependent attackers to execute arbitrary code via a crafted string. (CVE-2008-5557)

The page_uid and page_gid global variables are not properly initialized for use by the SAPI php_getuid function. This could allow context-dependent attackers to bypass safe_mode restrictions via variable settings. (CVE-2008-5624)

Certain versions of PHP do not enforce the error_log safe_mode restrictions when safe_mode is enabled. This could allow context-dependent attackers to write to arbitrary files. (CVE-2008-5625)

The ZipArchive::extractTo function in certain versions of PHP contains a directory traversal vulnerability. This could allow context-dependent attackers to write arbitrary files via a specially crafted ZIP file. (CVE-2008-5658)

Certain versions of PHP ship with a flawed implementation of magic_quotes_gpc. This could allow context-dependent attackers to conduct SQL injection attacks. (CVE-2008-5844)

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2008-10-09
APPLE	APPLE-SA-2009-05-12
BID	30087
BID	31681
BID	32383
BID	32625
BID	32673
BID	32688
BID	32948
CERT	TA09-133A
CVE	CVE-2008-2371
CVE	CVE-2008-5557
CVE	CVE-2008-5624
CVE	CVE-2008-5625
CVE	CVE-2008-5658
CVE	CVE-2008-5844
DEBIAN	DSA-1602
DEBIAN	DSA-1789

Source	Reference
OSVDB	50480
OSVDB	50483
OSVDB	52205
OSVDB	52207
OVAL	OVAL10286
REDHAT	RHSA-2009:0350
SECUNIA	30916
SECUNIA	30944
SECUNIA	30945
SECUNIA	30958
SECUNIA	30961
SECUNIA	30967
SECUNIA	30972
SECUNIA	30990
SECUNIA	31200
SECUNIA	32222
SECUNIA	32454
SECUNIA	34642
SECUNIA	35003
SECUNIA	35074
SECUNIA	35306
SECUNIA	35650
SECUNIA	39300
URL	http://bugs.php.net/bug.php?id=42718
URL	http://bugs.php.net/bug.php?id=45722
URL	http://www.php.net/ChangeLog-5.php#5.2.8
XF	php-error-safemode-bypass(47314)
XF	php-getuid-safemode-bypass(47318)
XF	php-multibyte-bo(47525)
XF	php-ziparchive-directory-traversal(47079)

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.8.tar.gz

Upgrade to PHP v5.2.8 (released on December 8th, 2008).

3.1.8. PHP Fixed security issue (php-fixed-security-issue)

Description:

The init_request_info function in sapi/cgi/cgi_main.c in PHP before 5.2.6 does not properly consider operator precedence when calculating the length of PATH_TRANSLATED, which might allow remote attackers to execute arbitrary code via a crafted URI.

Affected Nodes:

Affected Nodes:	**Additional Information:**
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	**Reference**
APPLE	APPLE-SA-2008-07-31
BID	29009
CERT-VN	147027
CVE	CVE-2008-0599
OVAL	OVAL5510
REDHAT	RHSA-2008:0505
SECUNIA	30048
SECUNIA	30083
SECUNIA	30345
SECUNIA	30616
SECUNIA	30757
SECUNIA	30828
SECUNIA	31200
SECUNIA	31326
SECUNIA	35650
XF	php-vector-unspecified(42137)

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.6.tar.gz
Upgrade to PHP v5.2.6.

3.1.9. VNC password is "password" (vnc-password-password)

Description:

The VNC server is using the password "password". This would allow anyone to log into the machine via VNC and take complete control.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:5900	Running vulnerable VNC service. Successfully authenticated to the VNC service with credentials: uid[null] pw[password] realm[null]

References:

None

Vulnerability Solution:

Change the password to a stronger, unpredictable one.

3.1.10. Samba GETDC Mailslot Processing Buffer Overflow In Nmbd (cifs-samba-nmbd-getdc-mailslot-bof)

Description:

Versions 3.0.0 through 3.0.26a (inclusive) of Samba, the Server Message Block protocol server are vulnerable to what is believed to be a non-exploitable buffer overflow in nmbd during the processing of GETDC logon server requests. This code is only used when the Samba server is configured as a Primary or Backup Domain Controller.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:139	Running vulnerable CIFS service: Samba 3.0.20-Debian.
192.168.56.3:445	Running vulnerable CIFS service: Samba 3.0.20-Debian.

References:

Source	Reference
APPLE	APPLE-SA-2007-12-17
BID	26454
CERT	TA07-352A
CVE	CVE-2007-4572
DEBIAN	DSA-1409
OVAL	OVAL11132
OVAL	OVAL5643
REDHAT	RHSA-2007:1013
REDHAT	RHSA-2007:1016
REDHAT	RHSA-2007:1017
SECUNIA	27450
SECUNIA	27679
SECUNIA	27682
SECUNIA	27691

Source	Reference
SECUNIA	27701
SECUNIA	27720
SECUNIA	27731
SECUNIA	27787
SECUNIA	27927
SECUNIA	28136
SECUNIA	28368
SECUNIA	29341
SECUNIA	30484
SECUNIA	30736
SECUNIA	30835
SUSE	SUSE-SA:2007:065
URL	http://samba.org/samba/security/CVE-2007-4572.html
XF	samba-nmbd-bo(38501)

Vulnerability Solution:

Download and apply the upgrade from: http://us1.samba.org/samba/ftp/old-versions/samba-3.0.27.tar.gz

3.1.11. Samba 'reply_netbios_packet' Nmbd Buffer Overflow (cifs-samba-reply-netbios-packet-bof)

Description:

Versions 3.0.0 through 3.0.26a (inclusive) of Samba, the Server Message Block protocol server are vulnerable to a buffer overflow in reply_netbios_packet() in nmbd when processing multiple specially crafted WINS "Name Registration" requests followed by a WINS "Name Query" request. This could allow a remote attacker to execute arbitrary code.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:139	Running vulnerable CIFS service: Samba 3.0.20-Debian.
192.168.56.3:445	Running vulnerable CIFS service: Samba 3.0.20-Debian.

References:

Source	Reference
APPLE	APPLE-SA-2007-12-17
BID	26455
CERT	TA07-352A
CVE	CVE-2007-5398
DEBIAN	DSA-1409
OVAL	OVAL10230

Source	Reference
OVAL	OVAL5811
REDHAT	RHSA-2007:1013
REDHAT	RHSA-2007:1016
REDHAT	RHSA-2007:1017
SECUNIA	27450
SECUNIA	27679
SECUNIA	27682
SECUNIA	27691
SECUNIA	27701
SECUNIA	27720
SECUNIA	27731
SECUNIA	27742
SECUNIA	27787
SECUNIA	27927
SECUNIA	28136
SECUNIA	28368
SECUNIA	29341
SECUNIA	30484
SECUNIA	30835
SUSE	SUSE-SA:2007:065
URL	http://samba.org/samba/security/CVE-2007-5398.html
URL	http://secunia.com/secunia_research/2007-90/advisory/
XF	samba-replynetbiospacket-bo(38502)

Vulnerability Solution:

Download and apply the upgrade from: http://us1.samba.org/samba/ftp/old-versions/samba-3.0.27.tar.gz

3.1.12. Samba send_mailslot GETDC Buffer Overflow (cifs-samba-send-mailslot-bof)

Description:

A buffer overflow within Samba's WINS server (nmbd) allows for the remote execution of arbitrary code. This defect is only exploitable when the "domain logons" parameter has been enabled in smb.conf.

The vulnerability is exploited by sending a malformed domain logon packet with an overly long GETDC string, causing a stack-based buffer overflow.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.56.3:139	Running vulnerable CIFS service: Samba 3.0.20-Debian.
192.168.56.3:445	Running vulnerable CIFS service: Samba 3.0.20-Debian.

References:

Source	Reference
APPLE	APPLE-SA-2008-02-11
BID	26791
CERT	TA08-043B
CERT-VN	438395
CVE	CVE-2007-6015
DEBIAN	DSA-1427
OVAL	OVAL11572
OVAL	OVAL5605
REDHAT	RHSA-2007:1114
REDHAT	RHSA-2007:1117
SECUNIA	27760
SECUNIA	27894
SECUNIA	27977
SECUNIA	27993
SECUNIA	27999
SECUNIA	28003
SECUNIA	28028
SECUNIA	28029
SECUNIA	28037
SECUNIA	28067
SECUNIA	28089
SECUNIA	28891
SECUNIA	29032
SECUNIA	29341
SECUNIA	30484
SECUNIA	30835
SUSE	SUSE-SA:2007:068
URL	http://secunia.com/advisories/27760/
URL	http://us1.samba.org/samba/security/CVE-2007-6015.html
XF	samba-sendmailslot-bo(38965)

Vulnerability Solution:

Download and apply the upgrade from: http://us1.samba.org/samba/ftp/old-versions/samba-3.0.28.tar.gz

3.1.13. Handling of zero length rdata can cause named to terminate unexpectedly (dns-bind-cve-2012-1667)

Description:

This problem was uncovered while testing with experimental DNS record types. It is possible to add records to BIND with null (zero length) rdata fields. Processing of these records may lead to unexpected outcomes. Recursive servers may crash or disclose some portion of memory to the client. Secondary servers may crash on restart after transferring a zone containing these records. Master servers may corrupt zone data if the zone option "auto-dnssec" is set to "maintain". Other unexpected problems that are not listed here may also be encountered. This issue primarily affects recursive nameservers. Authoritative nameservers will only be impacted if an administrator configures experimental record types with no data. If the server is configured this way, then secondaries can crash on restart after transferring that zone. Zone data on the master can become corrupted if the zone with those records has named configured to manage the DNSSEC key rotation.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:53	Running vulnerable DNS service: BIND 9.4.2.

References:

Source	Reference
CVE	CVE-2012-1667
IAVM	2012-A-0106

Vulnerability Solution:

- Upgrade to BIND version 9.6-ESV-R7-P1

  Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/cur/9.6/bind-9.6-ESV-R7-P1.tar.gz
  Upgrade to 9.6-ESV-R7-P1 version of ISC BIND Which was released on June 04, 2012. The source code and binaries for this release can be downloaded from bind's website.

- Upgrade to BIND version 9.7.6-P1

  Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/cur/9.7/bind-9.7.6-P1.tar.gz
  Upgrade to 9.7.6-P1 version of ISC BIND Which was released on June 04, 2012. The source code and binaries for this release can be downloaded from bind's website.

- Upgrade to BIND version 9.8.3-P1

  Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/cur/9.8/bind-9.8.3-P1.tar.gz
  Upgrade to 9.8.3-P1 version of ISC BIND Which was released on June 04, 2012. The source code and binaries for this release can be downloaded from bind's website.

- Upgrade to BIND version 9.9.1-P1

  Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/cur/9.9/bind-9.9.1-P1.tar.gz
  Upgrade to 9.9.1-P1 version of ISC BIND Which was released on June 04, 2012. The source code and binaries for this release can be downloaded from bind's website.

3.1.14. Obsolete ISC BIND installation (dns-bind-obsolete)

Description:

ISC BIND 4 and earlier, 8 and earlier, as well as 9.4-ESV-R5 and earlier are considered obsolete. ISC will not fix security bugs in these versions (even critical ones).

ISC BIND 9.5.2-P4,9.6.0,9.6.3 reached their end-of-life but continue to receive security fixes (only if critical, though).

ISC BIND versions 9.7.6-P1,9.8.3-P1,9.9.1-P1 are the only ones actively maintained. It is strongly recommended that you upgrade your BIND installation to one of these versions.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:53	Running vulnerable DNS service: BIND 9.4.2.

References:

Source	Reference
URL	http://www.isc.org/software/bind
URL	http://www.isc.org/software/bind/versions

Vulnerability Solution:

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.9.0b1/bind-9.9.0b1.tar.gz
The latest version of BIND is version 9.9.0b1, released on November 09, 2011.

3.1.15. MySQL dispatch_command() Multiple Format String Vulnerabilities (mysql-dispatch_command-multiple-format-string)

Description:

Multiple format string vulnerabilities in the dispatch_command function in libmysqld/sql_parse.cc in mysqld in MySQL 4.0.0 through 5.0.83 allow remote authenticated users to cause a denial of service (daemon crash) and possibly have unspecified other impact via format string specifiers in a database name in a (1) COM_CREATE_DB or (2) COM_DROP_DB request.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:3306	Running vulnerable MySQL service: MySQL 5.0.51a.

References:

Source	Reference
APPLE	APPLE-SA-2010-03-29-1
BID	35609
CVE	CVE-2009-2446
OSVDB	55734

Source	Reference
OVAL	OVAL11857
REDHAT	RHSA-2010:0110
SECUNIA	35767
SECUNIA	38517
XF	mysql-dispatchcommand-format-string(51614)

Vulnerability Solution:

MySQL >= 5.0.0 and < 5.0.84

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.0.html

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.1.16. 'rexec' Remote Execution Service Enabled (service-rexec)

Description:

The RSH remote execution service (rexec) is enabled. This is a legacy service often configured to blindly trust some hosts and IPs. The protocol also doesn't support encryption or any sort of strong authentication mechanism.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:512	Running vulnerable Remote Execution service.

References:

None

Vulnerability Solution:

Disable or firewall this service which usually runs on 512/tcp.

3.1.17. Apache HTTPD: APR-util XML DoS (CVE-2009-1955) (apache-httpd-cve-2009-1955)

Description:

The affected asset is vulnerable to this vulnerability ONLY if an attacker could convince Apache to consume a specially crafted XML document. Review your Web server configuration for validation.The affected asset is vulnerable to this vulnerability ONLY if an attacker could convince Apache to consume a specially crafted XML document. Review your Web server configuration for validation.A denial of service flaw was found in the bundled copy of the APR-util library Extensible Markup Language (XML) parser. A remote attacker could create a specially-crafted XML document that would cause excessive memory consumption when processed by the XML decoding engine.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
BID	35253
CVE	CVE-2009-1955
DEBIAN	DSA-1812
OVAL	OVAL10270
OVAL	OVAL12473
REDHAT	RHSA-2009:1107
REDHAT	RHSA-2009:1108
SECUNIA	34724
SECUNIA	35284
SECUNIA	35360
SECUNIA	35395
SECUNIA	35444
SECUNIA	35487
SECUNIA	35565
SECUNIA	35710
SECUNIA	35797
SECUNIA	35843
SECUNIA	36473
SECUNIA	37221
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.2 and < 2.2.12

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.1.18. Apache HTTPD: mod_proxy_ftp FTP command injection (CVE-2009-3095) (apache-httpd-cve-2009-3095)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running module mod_proxy_ftp. Review your Web server configuration for validation.A flaw was found in the mod_proxy_ftp module. In a reverse proxy configuration, a remote attacker could use this flaw to bypass intended access restrictions by creating a carefully-crafted HTTP Authorization header, allowing the attacker to send arbitrary commands to the FTP server.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2010-03-29-1
CVE	CVE-2009-3095
DEBIAN	DSA-1934
OVAL	OVAL8662
OVAL	OVAL9363
SECUNIA	37152
SUSE	SUSE-SA:2009:050
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache >= 2.2 and < 2.2.14

Upgrade to Apache HTTPD version 2.2.14

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.gz

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.1.19. VNC remote control service installed (backdoor-vnc-0001)

Description:

AT&T Virtual Network Computing (VNC) provides remote users with access to the system it is installed on. If this service is compromised, the user can gain complete control of the system.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:5900	Running vulnerable VNC service.

References:

None

Vulnerability Solution:

Remove or disable this service. If it is necessary, be sure to use well thought out (hard to crack) passwords. It is important to note that VNC truncates passwords to 8 bytes when authenticating, making it more susceptible to brute force attacks.
To protect data from eaves-droppers, tunneling VNC through SSH is recommended.
Additionally, restricting access to specific IP addresses using TCP wrappers is also recommended.
For more information on VNC, visit the VNC website.

3.1.20. CIFS NULL Session Permitted (cifs-nt-0001)

Description:

NULL sessions allow anonymous users to establish unauthenticated CIFS sessions with Windows or third-party CIFS implementations such as Samba or the Solaris CIFS Server. These anonymous users may be able to enumerate local users, groups, servers, shares, domains, domain policies, and may be able to access various MSRPC services through RPC function calls. These services have been historically affected by numerous vulnerabilities. The wealth of information available to attackers through NULL sessions may also allow them to carry out more sophisticated attacks.

Affected Nodes:

Affected Nodes:	**Additional Information:**
192.168.56.3	Found server name: METASPLOITABLEFound policy for domain(s): METASPLOITABLE Builtin

References:

Source	**Reference**
CVE	CVE-1999-0519
URL	http://www.hsc.fr/ressources/presentations/null_sessions/

Vulnerability Solution:

•Microsoft Windows 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003, Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003

Disable NULL sessions

Modify the registry key:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\`

with the following values:

```
Value Name: RestrictAnonymous
Data Type: REG_DWORD
Data Value: 1

Value Name: RestrictAnonymousSAM
Data Type: REG_DWORD
```

```
      Data Value: 1

      Value Name: EveryoneIncludesAnonymous
      Data Type: REG_DWORD
      Data Value: 0
```

and set the following value to 0 (or, alternatively, delete it):

```
      Value Name: TurnOffAnonymousBlock
      Data Type: REG_DWORD
      Data Value: 0
```

Modify the registry key:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\`

with the following values:

```
      Value Name: RestrictNullSessAccess
      Data Type: REG_DWORD
      Data Value: 1

      Value Name: NullSessionPipes
      Data Type: REG_MULTI_SZ
      Data Value: "" (empty string, without quotes)
```

Open Local Security Settings, and disable the following setting:

```
       Security Settings -> Local Policies -> Security Options ->
       Network access: Allow anonymous SID/Name translation: Disabled
```

Finally, reboot the machine.

Please note that disabling NULL sessions may have an adverse impact on functionality, as some applications and network environments may depend on them for proper operation. Refer to Microsoft Knowledge Base Article 823659 for more information.

•Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional

Disable NULL sessions

Modify the registry key:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\`

with the following values:

```
      Value Name: RestrictAnonymous
      Data Type: REG_DWORD
      Data Value: 1

      Value Name: RestrictAnonymousSAM
      Data Type: REG_DWORD
      Data Value: 1

      Value Name: EveryoneIncludesAnonymous
```

```
     Data Type: REG_DWORD
     Data Value: 0
```

Modify the registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\
```

with the following values:

```
     Value Name: RestrictNullSessAccess
     Data Type: REG_DWORD
     Data Value: 1

     Value Name: NullSessionPipes
     Data Type: REG_MULTI_SZ
     Data Value: "" (empty string, without quotes)
```

Open Local Security Settings, and disable the following setting:

```
      Security Settings -> Local Policies -> Security Options ->
      Network access: Allow anonymous SID/Name translation: Disabled
```

Finally, reboot the machine.

Please note that disabling NULL sessions may have an adverse impact on functionality, as some applications and network environments may depend on them for proper operation. Refer to Microsoft Knowledge Base Article Q246261 for more information.

- Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server

Disable NULL sessions

Modify the registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\
```

with the following value:

```
     Value Name: RestrictAnonymous
     Data Type: REG_DWORD
     Data Value: 2
```

After modifying the registry, reboot the machine.

Please note that disabling NULL sessions may have an adverse impact on functionality, as some applications and network environments may depend on them for proper operation. Refer to Microsoft Knowledge Base Article Q246261 for more information.

- Microsoft Windows NT Server 4.0, Microsoft Windows NT Server, Enterprise Edition 4.0, Microsoft Windows NT Workstation 4.0

Install Microsoft service pack Windows NT4 Service Pack 4

Download and apply the upgrade from: http://support.microsoft.com/sp

- Microsoft Windows NT, Microsoft Windows NT Workstation, Microsoft Windows NT Server, Microsoft Windows NT Advanced Server, Microsoft Windows NT Server, Enterprise Edition, Microsoft Windows NT Server, Terminal Server Edition

Disable NULL sessions

Modify the registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\
```

with the following value:

```
     Value Name: RestrictAnonymous
     Data Type: REG_DWORD
     Data Value: 1
```

After modifying the registry, reboot the machine.

It is important to note that on Windows NT 4.0 systems, setting this registry entry will still leave the system open to various attacks, including brute-force enumeration of users and groups. A complete solution for Windows NT 4.0 systems is not available.

•Samba on Linux

Restrict anonymous access

To restrict anonymous access to Samba, modify your "smb.conf" settings as follows:

```
                    guest account = nobody
                    restrict anonymous = 1
```

```
Note: Make sure you do NOT list a user "nobody" in your password file.
```

•Novell NetWare

Novell Netware CIFS

As of May 9, 2007 Novell Netware CIFS does not provide a workaround for this vulnerability.

3.1.21. Samba AFS Filesystem ACL Mapping Format String Vulnerability (cifs-samba-afs-filesystem-acl-mapping-bof)

Description:

Certain versions of Samba are vulnerable to a format string condition when handling ACL mapping operations on AFS file systems. Successful exploitation allows an authenticated attacker with write access to an AFS share to execute arbitrary code as the root user.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:139	Running vulnerable CIFS service: Samba 3.0.20-Debian.
192.168.56.3:445	Running vulnerable CIFS service: Samba 3.0.20-Debian.

References:

Source	Reference
BID	22403
CERT-VN	649732
CVE	CVE-2007-0454
DEBIAN	DSA-1257

Source	Reference
OSVDB	33101
SECUNIA	24021
SECUNIA	24046
SECUNIA	24060
SECUNIA	24067
SECUNIA	24101
SECUNIA	24145
SECUNIA	24151
URL	http://samba.org/samba/security/CVE-2007-0454.html
XF	samba-afsacl-format-string(32304)

Vulnerability Solution:

Download and apply the upgrade from: http://us1.samba.org/samba/ftp/old-versions/samba-3.0.24.tar.gz

3.1.22. Samba receive_smb_raw() Buffer Overflow (cifs-samba-receive-smb-raw-bof)

Description:

Versions 3.0.0 through 3.0.29a (inclusive) of Samba, the Server Message Block protocol server are vulnerable to a heap-based buffer overflow due to a calculation error in the receive_smb_raw() function. An attacker could construct a malicious SMB packet to exploit the vulnerability and execute arbitrary code under the context of the Samba server user.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:139	Running vulnerable CIFS service: Samba 3.0.20-Debian.
192.168.56.3:445	Running vulnerable CIFS service: Samba 3.0.20-Debian.

References:

Source	Reference
APPLE	APPLE-SA-2008-06-30
BID	29404
BID	31255
CVE	CVE-2008-1105
DEBIAN	DSA-1590
OVAL	OVAL10020
OVAL	OVAL5733
REDHAT	RHSA-2008:0288
REDHAT	RHSA-2008:0289
REDHAT	RHSA-2008:0290

Source	Reference
SECUNIA	30228
SECUNIA	30385
SECUNIA	30396
SECUNIA	30442
SECUNIA	30449
SECUNIA	30478
SECUNIA	30489
SECUNIA	30543
SECUNIA	30736
SECUNIA	30802
SECUNIA	30835
SECUNIA	31246
SECUNIA	31911
SECUNIA	33696
SUSE	SUSE-SA:2008:026
URL	http://samba.org/samba/security/CVE-2008-1105.html
URL	http://secunia.com/secunia_research/2008-20/advisory/
XF	samba-receivesmbraw-bo(42664)
XF	xerox-controller-samba-code-execution(45251)

Vulnerability Solution:

Download and apply the upgrade from: http://us1.samba.org/samba/ftp/old-versions/samba-3.0.30.tar.gz

3.1.23. PHP Multiple Vulnerabilities Fixed in version 5.2.11 (http-php-multiple-vulns-5-2-11)

Description:

Fixed certificate validation inside php_openssl_apply_verification_policy (CVE-2009-3291)

Added missing sanity checks around exif processing (CVE-2009-3292)

Fixed sanity check for the color index in imagecolortransparent (CVE-2009-3293)

Fixed bug #44683 (popen crashes when an invalid mode is passed)

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
CVE	CVE-2009-3291
CVE	CVE-2009-3292
CVE	CVE-2009-3293
DEBIAN	DSA-1940
OSVDB	58185
OSVDB	58186
OSVDB	58187
OVAL	OVAL10438
OVAL	OVAL7047
OVAL	OVAL7394
OVAL	OVAL7652
OVAL	OVAL9982
SECUNIA	36791
SECUNIA	37412
SECUNIA	37482
SECUNIA	40262
URL	http://bugs.php.net/44683
URL	http://www.php.net/ChangeLog-5.php#5.2.11
URL	http://www.php.net/releases/5_2_11.php
XF	php-certificate-unspecified(53334)

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.2.11.tar.gz/from/a/mirror

Upgrade to PHP v5.2.11 (released on September 16th, 2009).

3.1.24. PHP Multiple Vulnerabilities Fixed in version 5.2.13 (http-php-multiple-vulns-5-2-13)

Description:

Improved LCG entropy (CVE-2010-1128)

Fixed safe_mode validation inside tempnam() when the directory path does not end with a / (CVE-2010-1129)

Fixed a possible open_basedir/safe_mode bypass in the session extension identified by Grzegorz Stachowiak (CVE-2010-1130)

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2010-08-24-1
BID	38430
BID	38431
CVE	CVE-2010-1128
CVE	CVE-2010-1129
CVE	CVE-2010-1130
REDHAT	RHSA-2010:0919
SECUNIA	38708
SECUNIA	40551
SECUNIA	42410
URL	http://www.php.net/ChangeLog-5.php#5.2.13
URL	http://www.php.net/releases/5_2_13.php

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.2.13.tar.gz/from/a/mirror

Upgrade to PHP v5.2.13 (released on February 25th, 2010).

3.1.25. PHP Upgraded PCRE to version 7.8 (http-php-multiple-vulns-5-2-7)

Description:

Heap-based buffer overflow in pcre_compile.c in the Perl-Compatible Regular Expression (PCRE) library 7.7 allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a regular expression that begins with an option and contains multiple branches.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2008-10-09
APPLE	APPLE-SA-2009-05-12
BID	30087
BID	31681

Source	Reference
CERT	TA09-133A
CVE	CVE-2008-2371
DEBIAN	DSA-1602
SECUNIA	30916
SECUNIA	30944
SECUNIA	30945
SECUNIA	30958
SECUNIA	30961
SECUNIA	30967
SECUNIA	30972
SECUNIA	30990
SECUNIA	31200
SECUNIA	32222
SECUNIA	32454
SECUNIA	35074
SECUNIA	35650
SECUNIA	39300

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.7.tar.gz
Upgrade to PHP v5.2.7.

3.1.26. PHP Multiple Vulnerabilities Fixed in version 5.3.1 (http-php-multiple-vulns-5-3-1)

Description:

Added "max_file_uploads" INI directive, which can be set to limit the number of file uploads per-request to 20 by default, to prevent possible DOS via temporary file exhaustion.

Added missing sanity checks around exif processing.

Fixed a safe_mode bypass in tempnam().

Fixed a open_basedir bypass in posix_mkfifo().

Fixed bug #50063 (safe_mode_include_dir fails).

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
APPLE	APPLE-SA-2010-03-29-1
CVE	CVE-2009-3292
CVE	CVE-2009-3557
CVE	CVE-2009-3558
CVE	CVE-2009-3559
CVE	CVE-2009-4017
DEBIAN	DSA-1940
OSVDB	58186
OVAL	OVAL10483
OVAL	OVAL6667
OVAL	OVAL7396
OVAL	OVAL7652
OVAL	OVAL9982
SECUNIA	36791
SECUNIA	37412
SECUNIA	37482
SECUNIA	37821
SECUNIA	40262
SECUNIA	41480
SECUNIA	41490
URL	http://www.php.net/ChangeLog-5.php#5.3.1
URL	http://www.php.net/releases/5_3_1.php
XF	php-multipart-formdata-dos(54455)

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.3.1.tar.gz/from/a/mirror
Upgrade to PHP v5.3.1 (released on November 19th, 2009).

3.1.27. MySQL default account: root/no password (mysql-default-account-root-nopassword)

Description:

MySQL is installed with a default of no password on the root (superuser) account. The password on this account must be changed to prevent malicious users from logging into the MySQL database with superuser privileges.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:3306	Running vulnerable MySQL service. Successfully authenticated to the MySQL service with credentials: uid[root] pw[] realm[mysql]

References:

Source	Reference
BID	5503
CVE	CVE-2002-1809
XF	mysql-default-root-access(9902)

Vulnerability Solution:

The password should be changed to a non-default value. To change the password for the account, use the mysql command line tool to run the commands:

```
    UPDATE user SET password=password('new-password') WHERE user='user-name';
    FLUSH PRIVILEGES;
```

Where user-name should be replaced with the appropriate user name and new-password should be replaced with the new password.

3.1.28. MySQL yaSSL CertDecoder::GetName Multiple Buffer Overflows (mysql-yassl-certdecodergetname-multiple-bofs)

Description:

Multiple stack-based buffer overflows in the CertDecoder::GetName function in src/asn.cpp in TaoCrypt in yaSSL before 1.9.9, as used in mysqld in MySQL 5.0.x before 5.0.90, MySQL 5.1.x before 5.1.43, MySQL 5.5.x through 5.5.0-m2, and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption and daemon crash) by establishing an SSL connection and sending an X.509 client certificate with a crafted name field, as demonstrated by mysql_overflow1.py and the vd_mysql5 module in VulnDisco Pack Professional 8.11.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:3306	Running vulnerable MySQL service: MySQL 5.0.51a.

References:

Source	Reference
BID	37640
BID	37943
BID	37974
CVE	CVE-2009-4484
DEBIAN	DSA-1997

Source	Reference
OSVDB	61956
SECUNIA	37493
SECUNIA	38344
SECUNIA	38364
SECUNIA	38517
SECUNIA	38573
URL	http://bugs.mysql.com/bug.php?id=50227
URL	http://dev.mysql.com/doc/refman/5.0/en/news-5-0-90.html
URL	http://dev.mysql.com/doc/refman/5.1/en/news-5-1-43.html
XF	mysql-unspecified-bo(55416)

Vulnerability Solution:

•MySQL >= 5.0.0 and < 5.0.90

Upgrade to MySQL v5.0.90

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.0.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•MySQL >= 5.1.0 and < 5.1.43

Upgrade to MySQL v5.1.43

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.1.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.1.29. MySQL yaSSL Multiple Buffer Overflow Vulnerabilities (mysql-yassl-multiple-bof)

Description:

When configured with SSL support, MySQL 5.0.x before 5.0.54a, 5.1.x before 5.1.23, and 6.0.x before 6.0.4a is vulnerable to multiple buffer overflow vulnerabilities in the yaSSL package used to provide SSL support. The most severe of these vulnerabilities may allow unauthenticated remote code execution.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:3306	Running vulnerable MySQL service: MySQL 5.0.51a.

References:

Source	Reference
APPLE	APPLE-SA-2008-10-09
BID	27140

Source	Reference
BID	31681
CVE	CVE-2008-0226
CVE	CVE-2008-0227
DEBIAN	DSA-1478
SECUNIA	28324
SECUNIA	28419
SECUNIA	28597
SECUNIA	29443
SECUNIA	32222
URL	http://bugs.mysql.com/bug.php?id=33814
XF	yassl-hashwithtransformupdate-dos(39433)
XF	yassl-inputbufferoperator-bo(39431)
XF	yassl-processoldclienthello-bo(39429)

Vulnerability Solution:

•MySQL >= 5.0.0 and < 5.0.54a

Upgrade to MySQL v5.0.54a

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.0.html

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•MySQL (?:^5.1.)

Upgrade to MySQL v5.1.23

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.1.html

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•MySQL (?:^6.0.)

Upgrade to MySQL v6.0.4a

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/6.0.html

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.1.30. Debian's OpenSSL Library Predictable Random Number Generator (openssl-debian-weak-keys)

Description:

A weakness has been discovered in the random number generator used by OpenSSL on Debian and Ubuntu systems. As a result of this weakness, certain encryption keys are much more common than they should be, such that an attacker could guess the key through a brute-force attack given minimal knowledge of the system. This particularly affects the use of encryption keys in OpenSSH, OpenVPN and SSL certificates. This vulnerability only affects operating systems which are based on Debian. However, other systems can be indirectly affected if weak keys are imported into them.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:22	SSH public key with fingerprint 5656240F211DDEA72BAE61B1243DE8F3 is a known weak key

References:

Source	Reference
BID	29179
CERT	TA08-137A
CERT-VN	925211
CVE	CVE-2008-0166
DEBIAN	DSA-1571
DEBIAN	DSA-1576
SECUNIA	30136
SECUNIA	30220
SECUNIA	30221
SECUNIA	30231
SECUNIA	30239
SECUNIA	30249
URL	http://metasploit.com/users/hdm/tools/debian-openssl/
URL	http://wiki.debian.org/SSLkeys
URL	http://www.debian.org/security/2008/dsa-1571
URL	http://www.debian.org/security/2008/dsa-1576
URL	http://www.debian.org/security/key-rollover/
URL	http://www.ubuntu.com/usn/usn-612-1
URL	http://www.ubuntu.com/usn/usn-612-2
URL	http://www.ubuntu.com/usn/usn-612-3
URL	http://www.ubuntu.com/usn/usn-612-4
URL	http://www.ubuntu.com/usn/usn-612-5
URL	http://www.ubuntu.com/usn/usn-612-6
URL	http://www.ubuntu.com/usn/usn-612-7
URL	http://www.ubuntu.com/usn/usn-612-8
XF	openssl-rng-weak-security(42375)

Vulnerability Solution:

Upgrade the OpenSSL package to the version recomended below to fix the random number generator and stop generating weak keys

•For Debian 4.0 etch, upgrade to 0.9.8c-4etch3

•For Debian testing (lenny), upgrade to 0.9.8g-9

•For Debian unstable (sid), upgrade to 0.9.8g-9

•For Ubuntu 7.0.4 (feisty), upgrade to 0.9.8c-4ubuntu0.3

•For Ubuntu 7.10 (gusty), upgrade to 0.9.8e-5ubuntu3.2

•For Ubuntu 8.0.4 (hardy), upgrade to 0.9.8g-4ubuntu3.1

Then regenerate all cryptographic key material which has been created by vulnerable OpenSSL versions on Debian-based systems. Affected keys include SSH server and user keys, OpenVPN keys, DNSSEC keys, keys associated to X.509 certificates, etc.

Optionally, Debian and Ubuntu have released updated OpenSSH, OpenSSL and OpenVPN packages to automatically blacklist known weak keys. It is recomended to install these upgrades on all systems.

3.1.31. PHP crash inside gd with invalid fonts (php-crash-inside-gd-with-invalid-fonts)

Description:

Buffer overflow in the imageloadfont function in ext/gd/gd.c in PHP 4.4.x before 4.4.9 and PHP 5.2 before 5.2.6-r6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted font file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2009-05-12
BID	30649
CERT	TA09-133A
CVE	CVE-2008-3658
DEBIAN	DSA-1647
OSVDB	47484
OVAL	OVAL9724
REDHAT	RHSA-2009:0350
SECUNIA	31982
SECUNIA	32148
SECUNIA	32316
SECUNIA	32884
SECUNIA	33797
SECUNIA	35074
SECUNIA	35306

Source	Reference
XF	php-imageloadfont-dos(44401)

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.7.tar.gz
Upgrade to PHP v5.2.7.

3.1.32. PHP Fixed bug #61910 Fix PHP-CGI query string parameter vulnerability (php-cve-2012-1823)

Description:

sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
CERT-VN	520827
CVE	CVE-2012-1823
REDHAT	RHSA-2012:0546
REDHAT	RHSA-2012:0547
REDHAT	RHSA-2012:0568
SECUNIA	49014
SECUNIA	49065
SECUNIA	49087

Vulnerability Solution:

- Upgrade to PHP v5.3.12

  Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.12.tar.gz
  Upgrade to PHP v5.3.12.

- Upgrade to PHP v5.4.2

  Download and apply the upgrade from: http://museum.php.net/php5/php-5.4.2.tar.gz
  Upgrade to PHP v5.4.2.

3.1.33. PHP Fixed bug #61910 Improve fix for PHP-CGI query string parameter vulnerability (php-cve-2012-2311)

Description:

sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that contain a %3D sequence but no = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
CERT-VN	520827
CVE	CVE-2012-2311
SECUNIA	49014

Vulnerability Solution:

•Upgrade to PHP v5.3.13

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.13.tar.gz
Upgrade to PHP v5.3.13.

•Upgrade to PHP v5.4.3

Download and apply the upgrade from: http://museum.php.net/php5/php-5.4.3.tar.gz
Upgrade to PHP v5.4.3.

3.1.34. PHP Fixed bug #61065 (php-cve-2012-2386)

Description:

Integer overflow in the phar_parse_tarfile function in tar.c in the phar extension in PHP before 5.3.14 and 5.4.x before 5.4.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted tar file that triggers a heap-based buffer overflow.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
CVE	CVE-2012-2386
IAVM	2012-B-0061

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.4.4.tar.gz
Upgrade to PHP v5.4.4.

3.1.35. PHP Fixed SplObjectStorage unserialization problems (php-fixed-splobjectstorage-unserialization-problems)

Description:

Use-after-free vulnerability in the SplObjectStorage unserializer in PHP 5.2.x and 5.3.x through 5.3.2 allows remote attackers to execute arbitrary code or obtain sensitive information via serialized data, related to the PHP unserialize function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2010-08-24-1
BID	40948
CVE	CVE-2010-2225
DEBIAN	DSA-2089
SECUNIA	40860
XF	php-splobjectstorage-code-execution(59610)

Vulnerability Solution:

- Upgrade to PHP v5.2.14

  Download and apply the upgrade from: http://www.php.net/get/php-5.2.14.tar.gz/from/a/mirror
  Upgrade to PHP v5.2.14.

- Upgrade to PHP v5.3.3

  Download and apply the upgrade from: http://www.php.net/get/php-5.3.3.tar.gz/from/a/mirror
  Upgrade to PHP v5.3.3.

3.1.36. PHP Upgraded PCRE to version 7.8 (php-upgraded-pcre-to-version-7-8)

Description:

Heap-based buffer overflow in pcre_compile.c in the Perl-Compatible Regular Expression (PCRE) library 7.7 allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a regular expression that begins with an option and contains multiple branches.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2008-10-09
APPLE	APPLE-SA-2009-05-12
BID	30087
BID	31681
CERT	TA09-133A
CVE	CVE-2008-2371
DEBIAN	DSA-1602
SECUNIA	30916
SECUNIA	30944
SECUNIA	30945
SECUNIA	30958
SECUNIA	30961
SECUNIA	30967
SECUNIA	30972
SECUNIA	30990
SECUNIA	31200
SECUNIA	32222
SECUNIA	32454
SECUNIA	35074
SECUNIA	35650
SECUNIA	39300

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.7.tar.gz
Upgrade to PHP v5.2.7.

3.1.37. 'rlogin' Remote Login Service Enabled (service-rlogin)

Description:

The RSH remote login service (rlogin) is enabled. This is a legacy service often configured to blindly trust some hosts and IPs. The protocol also doesn't support encryption or any sort of strong authentication mechanism.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:513	Running vulnerable Remote Login service.

References:

Source	Reference
CVE	CVE-1999-0651

Vulnerability Solution:

Disable or firewall this service which usually runs on 513/tcp.

3.1.38. 'rsh' Remote Shell Service Enabled (service-rsh)

Description:

The RSH remote shell service (rsh) is enabled. This is a legacy service often configured to blindly trust some hosts and IPs. The protocol also doesn't support encryption or any sort of strong authentication mechanism.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:514	Running vulnerable Remote Shell service.

References:

Source	Reference
CVE	CVE-1999-0651

Vulnerability Solution:

Disable or firewall this service which usually runs on 514/tcp.

3.2. Severe Vulnerabilities

3.2.1. Apache HTTPD: mod_proxy reverse proxy DoS (CVE-2009-1890) (apache-httpd-cve-2009-1890)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running module mod_proxy. Review your Web server configuration for validation.A denial of service flaw was found in the mod_proxy module when it was used as a reverse proxy. A remote attacker could use this flaw to force a proxy process to consume large amounts of CPU time.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
BID	35565
CVE	CVE-2009-1890
DEBIAN	DSA-1834
OSVDB	55553
OVAL	OVAL12330
OVAL	OVAL8616
OVAL	OVAL9403
REDHAT	RHSA-2009:1148
REDHAT	RHSA-2009:1156
SECUNIA	35691
SECUNIA	35721
SECUNIA	35793
SECUNIA	35865
SECUNIA	37152
SECUNIA	37221
SUSE	SUSE-SA:2009:050
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.2 and < 2.2.12
Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.2. Apache HTTPD: mod_deflate DoS (CVE-2009-1891) (apache-httpd-cve-2009-1891)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running module mod_deflate. Review your Web server configuration for validation.A denial of service flaw was found in the mod_deflate module. This module continued to compress large files until compression was complete, even if the network connection that requested the content was closed before compression completed. This would cause mod_deflate to consume large amounts of CPU if mod_deflate was enabled for a large file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
CVE	CVE-2009-1891
DEBIAN	DSA-1834
OSVDB	55782
OVAL	OVAL12361
OVAL	OVAL8632
OVAL	OVAL9248
REDHAT	RHSA-2009:1148
REDHAT	RHSA-2009:1156
SECUNIA	35721
SECUNIA	35781
SECUNIA	35793
SECUNIA	35865
SECUNIA	37152
SECUNIA	37221
SUSE	SUSE-SA:2009:050
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache >= 2.2 and < 2.2.12

Upgrade to Apache HTTPD version 2.2.12

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.3. X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch)

Description:

The subject common name (CN) field in the X.509 certificate does not match the name of the entity presenting the certificate.

Before issuing a certificate, a Certification Authority (CA) must check the identity of the entity requesting the certificate, as specified in the CA's Certification Practice Statement (CPS). Thus, standard certificate validation procedures require the subject CN field of a certificate to match the actual name of the entity presenting the certificate. For example, in a certificate presented by "https://www.example.com/", the CN should be "www.example.com".

In order to detect and prevent active eavesdropping attacks, the validity of a certificate must be verified, or else an attacker could then launch a man-in-the-middle attack and gain full control of the data stream. Of particular importance is the validity of the subject's CN, that should match the name of the entity (hostname).

A CN mismatch most often occurs due to a configuration error, though it can also indicate that a man-in-the-middle attack is being conducted.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:25	The subject common name found in the X.509 certificate ('CN=ubuntu804-base.localdomain') does not seem to match the scan target '192.168.56.3': Subject CN 'ubuntu804-base.localdomain' does not match node name '192.168.56.3'

References:

None

Vulnerability Solution:

The subject's common name (CN) field in the X.509 certificate should be fixed to reflect the name of the entity presenting the certificate (e.g., the hostname). This is done by generating a new certificate usually signed by a Certification Authority (CA) trusted by both the client and server.

3.2.4. Samba File Renaming Denial of Service Vulnerability (cifs-samba-file-renaming-dos)

Description:

Certain versions of Samba are vulnerable to a denial of service condition when handling deferred file open operations during file renaming requests. Successful exploitation allows an authenticated attacker to put the daemon in an infinite loop, causing all functionality to halt.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:139	Running vulnerable CIFS service: Samba 3.0.20-Debian.
192.168.56.3:445	Running vulnerable CIFS service: Samba 3.0.20-Debian.

References:

Source	Reference
BID	22395

Source	Reference
CVE	CVE-2007-0452
DEBIAN	DSA-1257
OSVDB	33100
OVAL	OVAL9758
REDHAT	RHSA-2007:0060
REDHAT	RHSA-2007:0061
SECUNIA	24021
SECUNIA	24030
SECUNIA	24046
SECUNIA	24060
SECUNIA	24067
SECUNIA	24076
SECUNIA	24101
SECUNIA	24140
SECUNIA	24145
SECUNIA	24151
SECUNIA	24188
SECUNIA	24284
SECUNIA	24792
SGI	20070201-01-P
SUSE	SUSE-SA:2007:016
URL	http://samba.org/samba/security/CVE-2007-0452.html
XF	samba-smbd-filerename-dos(32301)

Vulnerability Solution:

Download and apply the upgrade from: http://us1.samba.org/samba/ftp/old-versions/samba-3.0.24.tar.gz

3.2.5. SMB signing disabled (cifs-smb-signing-disabled)

Description:

This system does not allow SMB signing. SMB signing allows the recipient of SMB packets to confirm their authenticity and helps prevent man in the middle attacks against SMB. SMB signing can be configured in one of three ways: disabled entirely (least secure), enabled, and required (most secure).

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:139	Negotiate protocol response's security mode 3 indicates that SMB signing is

Affected Nodes:	Additional Information:
	disabled
192.168.56.3:445	Negotiate protocol response's security mode 3 indicates that SMB signing is disabled

References:

Source	Reference
URL	http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx

Vulnerability Solution:

•Microsoft Windows

Configure SMB signing

Configure the system to enable or require SMB signing as appropriate. The method for doing this is system specific so please see KB 887429 for details. Note: ensure that SMB signing configuration is done for incoming connections (Server).

•Samba

Configure SMB signing

Configure Samba to enable or require SMB signing as appropriate. To enable SMB signing, put the following in the Samba configuration file, typically smb.conf, in the global section:

```
server signing = auto
```

To require SMB signing, put the following in the Samba configuration file, typically smb.conf, in the global section:

```
server signing = mandatory
```

3.2.6. PHP Multiple Vulnerabilities Fixed in version 5.2.5 (http-php-multiple-vulns-5-2-5)

Description:

Various iconv_*() functions allow context-dependent attackers to cause a denial of service (application crash) via a long arguments (CVE-2007-4840, CVE-2007-4783).

The dl() function allows context-dependent attackers to cause a denial of service (application crash) via a long string in the library parameter. (CVE-2007-4887).

htmlentities/htmlspecialchars accept partial multibyte sequences (CVE-2007-5898).

The automatic session id insertion feature in output_add_rewrite_var() adds the session id to non-local forms (CVE-2007-5899).

Values set with php_admin_* in httpd.conf can be overwritten with ini_set() (CVE-2007-5900).

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
CVE	CVE-2007-5898
CVE	CVE-2007-5899
CVE	CVE-2007-5900
DEBIAN	DSA-1444
OSVDB	38918
OVAL	OVAL10080
OVAL	OVAL11211
REDHAT	RHSA-2008:0505
REDHAT	RHSA-2008:0544
REDHAT	RHSA-2008:0545
REDHAT	RHSA-2008:0546
REDHAT	RHSA-2008:0582
SECUNIA	27648
SECUNIA	27659
SECUNIA	27864
SECUNIA	28249
SECUNIA	28658
SECUNIA	30040
SECUNIA	30828
SECUNIA	31119
SECUNIA	31124
SECUNIA	31200
SUSE	SUSE-SA:2008:004
URL	http://www.php.net/releases/5_2_5.php

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.5.tar.gz
Upgrade to PHP v5.2.5.

3.2.7. MySQL Directory Traversal and Arbitrary Table Access Vulnerability (mysql-directory-traversal-and-arbitrary-table-access)

Description:

Directory traversal vulnerability in MySQL 5.0 before 5.0.91 and 5.1 before 5.1.47 allows remote authenticated users to bypass intended table grants to read field definitions of arbitrary tables, and on 5.1 to read or delete content of arbitrary tables, via a .. (dot dot) in a table name.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:3306	Running vulnerable MySQL service: MySQL 5.0.51a.

References:

Source	Reference
APPLE	APPLE-SA-2010-11-10-1
CVE	CVE-2010-1848
OVAL	OVAL10258
OVAL	OVAL7210
REDHAT	RHSA-2010:0442
REDHAT	RHSA-2010:0824
URL	http://bugs.mysql.com/bug.php?id=53371
URL	http://dev.mysql.com/doc/refman/5.0/en/news-5-0-91.html
URL	http://dev.mysql.com/doc/refman/5.1/en/news-5-1-47.html

Vulnerability Solution:

•MySQL >= 5.0.0 and < 5.0.91

Upgrade to MySQL v5.0.91

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.0.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•MySQL >= 5.1.0 and < 5.1.47

Upgrade to MySQL v5.1.47

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.1.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.8. MySQL vio_verify_callback() Zero-Depth X.509 Certificate Vulnerability (mysql-vio_verify_callback-zero-depth-x-509-certificate)

Description:

The vio_verify_callback function in viosslfactories.c in MySQL 5.0.x before 5.0.88 and 5.1.x before 5.1.41 accepts a value of zero for the depth of X.509 certificates when OpenSSL is used. This allows man-in-the-middle attackers to spoof arbitrary SSL-based MySQL servers via a crafted certificate.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:3306	Running vulnerable MySQL service: MySQL 5.0.51a.

References:

Source	Reference
CVE	CVE-2009-4028
OVAL	OVAL10940
OVAL	OVAL8510
REDHAT	RHSA-2010:0109
URL	http://bugs.mysql.com/bug.php?id=47320
URL	http://dev.mysql.com/doc/refman/5.0/en/news-5-0-88.html
URL	http://dev.mysql.com/doc/refman/5.1/en/news-5-1-41.html

Vulnerability Solution:

•MySQL >= 5.0.0 and < 5.0.88

Upgrade to MySQL v5.0.88

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.0.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•MySQL >= 5.1.0 and < 5.1.41

Upgrade to MySQL v5.1.41

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.1.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.9. X.509 Server Certificate Is Invalid/Expired (tls-server-cert-expired)

Description:

The TLS/SSL server's X.509 certificate either contains a start date in the future or is expired. Please refer to the proof in the section below for more details.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:25	The certificate is not valid after Sat, 17 Apr 2010 00:07:45 EST

References:

None

Vulnerability Solution:

Obtain a new certificate and install it on the server. The exact instructions for obtaining a new certificate depend on your organization's requirements. Generally, you will need to generate a certificate request and save the request as a file. This file is then sent to a Certificate Authority (CA) for processing. Please ensure that the start date and the end date on the new certificate are valid.

Your organization may have its own internal Certificate Authority. If not, you may have to pay for a certificate from a trusted external Certificate Authority.

After you have received a new certificate file from the Certificate Authority, you will have to install it on the TLS/SSL server. The exact instructions for installing a certificate differ for each product. Follow their documentation.

3.2.10. Apache HTTPD: APR-util off-by-one overflow (CVE-2009-1956) (apache-httpd-cve-2009-1956)

Description:

The affected asset is vulnerable to this vulnerability ONLY if an attacker can provide a specially crafted string to a function that handles a variable list of arguments on big-endian platforms. Review your Web server configuration for validation.The affected asset is vulnerable to this vulnerability ONLY if an attacker can provide a specially crafted string to a function that handles a variable list of arguments on big-endian platforms. Review your Web server configuration for validation.An off-by-one overflow flaw was found in the way the bundled copy of the APR-util library processed a variable list of arguments. An attacker could provide a specially-crafted string as input for the formatted output conversion routine, which could, on big-endian platforms, potentially lead to the disclosure of sensitive information or a denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
BID	35251
CVE	CVE-2009-1956
OVAL	OVAL11567
OVAL	OVAL12237
REDHAT	RHSA-2009:1107
REDHAT	RHSA-2009:1108
SECUNIA	34724
SECUNIA	35284
SECUNIA	35395
SECUNIA	35487
SECUNIA	35565
SECUNIA	35710
SECUNIA	35797
SECUNIA	35843

Source	Reference
SECUNIA	37221
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.2 and < 2.2.12
Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.11. Samba MS-RPC Shell Command Injection Vulnerability (cifs-samba-shell-command-injection-vuln)

Description:

Certain versions of Samba are vulnerable to a shell command injection when handling MS-RPC requests related to password changing, remote printing, and file share management. Successful exploitation allows an unauthenticated attacker to execute arbitrary commands as root.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:139	Running vulnerable CIFS service: Samba 3.0.20-Debian.
192.168.56.3:445	Running vulnerable CIFS service: Samba 3.0.20-Debian.

References:

Source	Reference
APPLE	APPLE-SA-2007-07-31
BID	23972
BID	25159
CERT-VN	268336
CVE	CVE-2007-2447
DEBIAN	DSA-1291
OSVDB	34700
OVAL	OVAL10062
REDHAT	RHSA-2007:0354
SECUNIA	25232
SECUNIA	25241
SECUNIA	25246
SECUNIA	25251
SECUNIA	25255
SECUNIA	25256

Source	Reference
SECUNIA	25257
SECUNIA	25259
SECUNIA	25270
SECUNIA	25289
SECUNIA	25567
SECUNIA	25675
SECUNIA	25772
SECUNIA	26083
SECUNIA	26235
SECUNIA	26909
SECUNIA	27706
SECUNIA	28292
SUSE	SUSE-SA:2007:031
URL	http://samba.org/samba/security/CVE-2007-2447.html

Vulnerability Solution:

Download and apply the upgrade from: http://us1.samba.org/samba/ftp/old-versions/samba-3.0.25.tar.gz

3.2.12. CIFS Share Writeable By Everyone (cifs-share-world-writeable)

Description:

A share was found which allows write access by anyone. The impact of this vulnerability could include:

•Total system compromise (if the share point allows write access to critical system files)

•Untraceable modification of important data

•Denial of service by filling up the disk

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3	Successfully opened share "tmp" with write permissions.

References:

Source	Reference
CVE	CVE-1999-0520

Vulnerability Solution:

Adjust the share permissions to restrict access to only those members of the organization who need the data. It is considered bad practice to grant the "Everyone", "Guest", or "Authenticated Users" groups read or write access to a share.

3.2.13. SMB signing not required (cifs-smb-signing-not-required)

Description:

This system enables, but does not require SMB signing. SMB signing allows the recipient of SMB packets to confirm their authenticity and helps prevent man in the middle attacks against SMB. SMB signing can be configured in one of three ways: disabled entirely (least secure), enabled, and required (most secure).

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:139	Negotiate protocol response's security mode 3 indicates that SMB signing is not required
192.168.56.3:445	Negotiate protocol response's security mode 3 indicates that SMB signing is not required

References:

Source	Reference
URL	http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx

Vulnerability Solution:

•Microsoft Windows

Configure SMB signing

Configure the system to enable or require SMB signing as appropriate. The method for doing this is system specific so please see KB 887429 for details. Note: ensure that SMB signing configuration is done for incoming connections (Server).

•Samba

Configure SMB signing

Configure Samba to enable or require SMB signing as appropriate. To enable SMB signing, put the following in the Samba configuration file, typically smb.conf, in the global section:

```
server signing = auto
```

To require SMB signing, put the following in the Samba configuration file, typically smb.conf, in the global section:

```
server signing = mandatory
```

3.2.14. BIND: Key algorithm rollover bug in bind9 (dns-bind-cve-2010-3614)

Description:

named, acting as a DNSSEC validator, was determining if an NS RRset is insecure based on a value that could mean either that the RRset is actually insecure or that there wasn't a matching key for the RRSIG in the DNSKEY RRset when resuming from validating the DNSKEY RRset. This can happen when in the middle of a DNSKEY algorithm rollover, when two different algorithms were used to sign a zone but only the new set of keys are in the zone DNSKEY RRset. See http://tools.ietf.org/html/draft-ietfdnsop-rfc4641bis-02#section-4.2.4 for example scenario.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:53	Running vulnerable DNS service: BIND 9.4.2.

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
BID	45137
CERT-VN	837744
CVE	CVE-2010-3614
DEBIAN	DSA-2130
OSVDB	69559
REDHAT	RHSA-2010:0975
REDHAT	RHSA-2010:0976
SECUNIA	42435
SECUNIA	42459
SECUNIA	42522
SECUNIA	42671

Vulnerability Solution:

•Upgrade to BIND version 9.4-ESV-R4

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.4-ESV-R4/bind-9.4-ESV-R4.tar.gz
Upgrade to 9.4-ESV-R4 version of ISC BIND Which was released on December 01, 2010. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.6-ESV-R3

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.6-ESV-R3/bind-9.6-ESV-R3.tar.gz
Upgrade to 9.6-ESV-R3 version of ISC BIND Which was released on December 01, 2010. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.6.2-P3

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.6.2-P3/bind-9.6.2-P3.tar.gz
Upgrade to 9.6.2-P3 version of ISC BIND Which was released on December 01, 2010. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.7.2-P3

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.7.2-P3/bind-9.7.2-P3.tar.gz
Upgrade to 9.7.2-P3 version of ISC BIND Which was released on December 01, 2010. The source code and binaries for this release can be downloaded from bind's website.

3.2.15. Insufficient DNS Source Port Randomization (dns-kaminsky-bug)

Description:

The DNS protocol, as implemented by most DNS servers and clients, allows remote attackers to spoof DNS traffic by predicting the source UDP port of a DNS request, and by bruteforcing the random 16-bit DNS transaction ID. Indeed, as demonstrated by Dan Kaminsky at Black Hat 2008 in Las Vegas, attackers can use various techniques to repeatedly attempt to guess the correct transaction ID. For example requests for multiple random hostnames can be sent to a recursive resolver; because these hostnames are unlikely to be already present in the resolver's cache, each request provides an opportunity for the attacker to bruteforce the transaction ID. Spoofed replies are then typically sent with in-bailiwick referrals to NS records chosen by the attacker,giving him complete control of entire domains. DNS clients as well as caching name servers are affected. Authoritative name servers are not.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:53	Running vulnerable DNS service: BIND 9.4.2.

References:

Source	Reference
APPLE	APPLE-SA-2008-07-31
APPLE	APPLE-SA-2008-09-09
APPLE	APPLE-SA-2008-09-12
APPLE	APPLE-SA-2008-09-15
BID	30131
CERT	TA08-190A
CERT	TA08-190B
CERT	TA08-260A
CERT-VN	800113
CVE	CVE-2008-1447
DEBIAN	DSA-1603
DEBIAN	DSA-1604
DEBIAN	DSA-1605
DEBIAN	DSA-1619
DEBIAN	DSA-1623
IAVM	2008-A-0044
IAVM	2008-A-0045
MS	MS08-037
NETBSD	NetBSD-SA2008-009
OVAL	OVAL12117

Source	Reference
OVAL	OVAL5725
OVAL	OVAL5761
OVAL	OVAL5917
OVAL	OVAL9627
REDHAT	RHSA-2008:0533
REDHAT	RHSA-2008:0789
SECUNIA	30925
SECUNIA	30973
SECUNIA	30977
SECUNIA	30979
SECUNIA	30980
SECUNIA	30988
SECUNIA	30989
SECUNIA	30998
SECUNIA	31011
SECUNIA	31012
SECUNIA	31014
SECUNIA	31019
SECUNIA	31022
SECUNIA	31030
SECUNIA	31031
SECUNIA	31033
SECUNIA	31052
SECUNIA	31065
SECUNIA	31072
SECUNIA	31093
SECUNIA	31094
SECUNIA	31137
SECUNIA	31143
SECUNIA	31151
SECUNIA	31152
SECUNIA	31153
SECUNIA	31169
SECUNIA	31197
SECUNIA	31199

Source	Reference
SECUNIA	31204
SECUNIA	31207
SECUNIA	31209
SECUNIA	31212
SECUNIA	31213
SECUNIA	31221
SECUNIA	31236
SECUNIA	31237
SECUNIA	31254
SECUNIA	31326
SECUNIA	31354
SECUNIA	31422
SECUNIA	31430
SECUNIA	31451
SECUNIA	31482
SECUNIA	31495
SECUNIA	31588
SECUNIA	31687
SECUNIA	31823
SECUNIA	31882
SECUNIA	31900
SECUNIA	33178
SECUNIA	33714
SECUNIA	33786
SUSE	SUSE-SA:2008:033
URL	http://isc.sans.org/diary.html?storyid=4687
URL	http://www.doxpara.com/?p=1176
XF	cisco-multiple-dns-cache-poisoning(43637)
XF	win-dns-client-server-spoofing(43334)

Vulnerability Solution:

•Upgrade to BIND version 9.3.5-P1

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.3.5-P1/bind-9.3.5-P1.tar.gz
Upgrade to 9.3.5-P1 version of ISC BIND Which was released on July 08, 2008. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.4.2-P1

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.4.2-P1/bind-9.4.2-P1.tar.gz

Upgrade to 9.4.2-P1 version of ISC BIND Which was released on July 08, 2008. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.5.0-P1

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.5.0-P1/bind-9.5.0-P1.tar.gz
Upgrade to 9.5.0-P1 version of ISC BIND Which was released on July 08, 2008. The source code and binaries for this release can be downloaded from bind's website.

3.2.16. FTP server does not support AUTH command (ftp-generic-0007)

Description:

FTP clients send credentials (user ID and password) in clear text to the FTP server by default. This allows malicious users to intercept the credentials if they can eavesdrop on the connection.

Newer FTP servers support the AUTH command, which provides enhanced authentication options such as TLS, Kerberos, GSSAPI, etc. This should be used to prevent eavesdropping on FTP connections.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:21	Server supports none of the following AUTH mechanisms: TLS TLS-C KERBEROS_V4 GSSAPI SSL

References:

None

Vulnerability Solution:

Upgrade/migrate to a FTP server that supports the AUTH command.

3.2.17. HTTP TRACE Method Enabled (http-trace-method-enabled)

Description:

The HTTP TRACE method is normally used to return the full HTTP request back to the requesting client for proxy-debugging purposes. An attacker can create a webpage using XMLHTTP, ActiveX, or XMLDOM to cause a client to issue a TRACE request and capture the client's cookies. This effectively results in a Cross-Site Scripting attack.

Affected Nodes:

Affected Nodes:	Additional Information:

192.168.56.3:80	Running vulnerable HTTP service.
	http://192.168.56.3/
	`3: TRACE / HTTP/1.1`
	`4: Host: 192.168.56.3`
	`3: Cookie: vulnerable=yes`

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
BID	15222
BID	19915
BID	24456
BID	36956
BID	9506
CERT-VN	867593
CVE	CVE-2004-2320
CVE	CVE-2004-2763
CVE	CVE-2005-3398
CVE	CVE-2006-4683
CVE	CVE-2007-3008
CVE	CVE-2008-7253
CVE	CVE-2009-2823
CVE	CVE-2010-0386
OSVDB	35511
OSVDB	3726
OVAL	OVAL1445
SECUNIA	10726
SECUNIA	17334
SECUNIA	21802
SECUNIA	25636
URL	http://www.apacheweek.com/issues/03-01-24#news
URL	http://www.kb.cert.org/vuls/id/867593
XF	mbedthis-httptrace-xss(34854)
XF	weblogic-trace-xss(14959)

Vulnerability Solution:

•Apache

Disable HTTP TRACE Method for Apache

Newer versions of Apache (1.3.34 and 2.0.55 and later) provide a configuration directive called TraceEnable. To deny TRACE requests, add the following line to the server configuration:

```
TraceEnable off
```

For older versions of the Apache webserver, use the mod_rewrite module to deny the TRACE requests:

```
RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^TRACE
RewriteRule .* - [F]
```

•IIS, PWS, Microsoft-IIS, Internet Information Services, Internet Information Services, Microsoft-PWS

Disable HTTP TRACE Method for Microsoft IIS

For Microsoft Internet Information Services (IIS), you may use the URLScan tool, freely available at http://www.microsoft.com/technet/security/tools/urlscan.mspx

•Java System Web Server, SunONE WebServer, Sun-ONE-Web-Server, iPlanet

Disable HTTP TRACE Method for SunONE/iPlanet

•For Sun ONE/iPlanet Web Server v6.0 SP2 and later, add the following configuration to the top of the default object in the 'obj.conf' file:

```
<Client method="TRACE">
  AuthTrans fn="set-variable"
     remove-headers="transfer-encoding"
     set-headers="content-length: -1"
     error="501"
</Client>
```

You must then restart the server for the changes to take effect.

•For Sun ONE/iPlanet Web Server prior to v6.0 SP2, follow the instructions provided the 'Relief/Workaround' section of Sun's official advisory: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603

•Lotus Domino

Disable HTTP TRACE Method for Domino

Follow IBM's instructions for disabling HTTP methods on the Domino server by adding the following line to the server's NOTES.INI file:

```
HTTPDisableMethods=TRACE
```

After saving NOTES.INI, restart the Notes web server by issuing the console command "tell http restart".

3.2.18. MySQL Bug #29801: Remote Federated Engine Crash (mysql-bug-29801-remote-federated-engine-crash)

Description:

Versions of MySQL server before 5.0.52 and 5.1.23 suffer from a denial of service vulnerability via a flaw in the federated engine. On issuance of a command to a remote server (e.g., SHOW TABLE STATUS LIKE 'table'), the local federated server expects a query to contain fourteen columns. A response with less than fourteen columns causes the federated server to crash.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:3306	Running vulnerable MySQL service: MySQL 5.0.51a.

References:

Source	Reference
URL	http://bugs.mysql.com/bug.php?id=29801

Vulnerability Solution:

•MySQL >= 5.0.0 and < 5.0.52

Upgrade to MySQL v5.0.52

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.0.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•MySQL (?:^5.1.)

Upgrade to MySQL v5.1.23

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.1.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.19. MySQL Bug #32707: send_error() Buffer Overflow Vulnerability (mysql-bug-32707-send-error-bof)

Description:

A buffer overflow in MySQL 5.0 through 5.0.54 and 5.1 before 5.1.23 contains a flaw in the protocol layer. A long error message can cause a buffer overflow, potentially leading to execution of code.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:3306	Running vulnerable MySQL service: MySQL 5.0.51a.

References:

Source	Reference
URL	http://bugs.mysql.com/bug.php?id=32707

Vulnerability Solution:

•MySQL >= 5.0.0 and < 5.0.54

Upgrade to MySQL v5.0.54

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.0.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•MySQL (?:^5.1.)

Upgrade to MySQL v5.1.23

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.1.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.20. MySQL Bug #37428: User-Defind Function Remote Code Execution (mysql-bug-37428-user-defind-function-remote-codex)

Description:

MySQL server 5.0 before 5.0.67 contains a flaw in creating and dropping certain functions. Using MySQL's user-defined functions, an authenticated attacker can create a function in a shared library and run arbitrary code against the server.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:3306	Running vulnerable MySQL service: MySQL 5.0.51a.

References:

Source	Reference
URL	http://bugs.mysql.com/bug.php?id=37428

Vulnerability Solution:

MySQL >= 5.0.0 and < 5.0.67
Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.0.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.21. MySQL Bug #38296: Nested Boolean Query Exhaustion Denial of Service (mysql-bug-38296-nested-boolean-query-exhaustion-dos)

Description:

There is a flaw in parsing queries in MySQL 5.0 before 5.0.68 and MySQL 5.1 before 5.1.28. An attacker can potentially cause the server to crash by sending a query with multiple nested logic operators, e.g. 'SELECT * FROM TABLE WHERE ... OR (... OR (... OR (...' etc.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:3306	Running vulnerable MySQL service: MySQL 5.0.51a.

References:

Source	Reference
URL	http://bugs.mysql.com/bug.php?id=38296

Vulnerability Solution:

- MySQL >= 5.0.0 and < 5.0.68

  Upgrade to MySQL v5.0.68

  Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.0.html
  Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

- MySQL >= 5.1.0 and < 5.1.28

Upgrade to MySQL v5.1.28

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.1.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.22. MySQL COM_FIELD_LIST Command Buffer Overflow Vulnerability (mysql-com_field_list-command-bof)

Description:

A buffer overflow in MySQL 5.0 before 5.0.91 and 5.1 before 5.1.47 allows remote authenticated users to execute arbitrary code via a COM_FIELD_LIST command with a long table name.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:3306	Running vulnerable MySQL service: MySQL 5.0.51a.

References:

Source	Reference
APPLE	APPLE-SA-2010-11-10-1
CVE	CVE-2010-1850
OVAL	OVAL10846
OVAL	OVAL6693
REDHAT	RHSA-2010:0442
URL	http://bugs.mysql.com/bug.php?id=53237
URL	http://dev.mysql.com/doc/refman/5.0/en/news-5-0-91.html
URL	http://dev.mysql.com/doc/refman/5.1/en/news-5-1-47.html

Vulnerability Solution:

•MySQL >= 5.0.0 and < 5.0.91

Upgrade to MySQL v5.0.91

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.0.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•MySQL >= 5.1.0 and < 5.1.47

Upgrade to MySQL v5.1.47

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.1.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.23. PHP possible overflow inside memnstr (php-possible-overflow-inside-memnstr)

Description:

Buffer overflow in the memnstr function in PHP 4.4.x before 4.4.9 and PHP 5.6 through 5.2.6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via the delimiter argument to the explode function. NOTE: the scope of this issue is limited since most applications would not use an attacker-controlled delimiter, but local attacks against safe_mode are feasible.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2009-05-12
CERT	TA09-133A
CVE	CVE-2008-3659
DEBIAN	DSA-1647
OSVDB	47483
SECUNIA	31982
SECUNIA	32148
SECUNIA	32316
SECUNIA	35074
SECUNIA	35650
XF	php-memnstr-bo(44405)

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.7.tar.gz
Upgrade to PHP v5.2.7.

3.2.24. Apache HTTPD: mod_proxy_http DoS (CVE-2008-2364) (apache-httpd-cve-2008-2364)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running module mod_proxy_http. Review your Web server configuration for validation.A flaw was found in the handling of excessive interim responses from an origin server when using mod_proxy_http. A remote attacker could cause a denial of service or high memory usage.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2008-10-09
BID	29653
BID	31681
CVE	CVE-2008-2364
OVAL	OVAL11713
OVAL	OVAL6084
OVAL	OVAL9577
REDHAT	RHSA-2008:0966
REDHAT	RHSA-2008:0967
SECUNIA	30621
SECUNIA	31026
SECUNIA	31404
SECUNIA	31416
SECUNIA	31651
SECUNIA	31904
SECUNIA	32222
SECUNIA	32685
SECUNIA	32838
SECUNIA	33156
SECUNIA	33797
SECUNIA	34219
SECUNIA	34259
SECUNIA	34418
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html
XF	apache-modproxy-module-dos(42987)

Vulnerability Solution:

•Apache >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache >= 2.2 and < 2.2.9

Upgrade to Apache HTTPD version 2.2.9

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.9.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.25. Apache HTTPD: AllowOverride Options handling bypass (CVE-2009-1195) (apache-httpd-cve-2009-1195)

Description:

The affected asset is vulnerable to this vulnerability ONLY if the AllowOverride directive with certin Options are used. Review your Web server configuration for validation.The affected asset is vulnerable to this vulnerability ONLY if the AllowOverride directive with certin Options are used. Review your Web server configuration for validation.A flaw was found in the handling of the "Options" and "AllowOverride" directives. In configurations using the "AllowOverride" directive with certain "Options=" arguments, local users were not restricted from executing commands from a Server-Side-Include script as intended.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
BID	35115
CVE	CVE-2009-1195
DEBIAN	DSA-1816
OSVDB	54733
OVAL	OVAL11094
OVAL	OVAL12377
OVAL	OVAL8704
REDHAT	RHSA-2009:1075
REDHAT	RHSA-2009:1156
SECUNIA	35261
SECUNIA	35264
SECUNIA	35395
SECUNIA	35453
SECUNIA	35721
SECUNIA	37152

Source	Reference
SUSE	SUSE-SA:2009:050
URL	http://httpd.apache.org/security/vulnerabilities_22.html
XF	apache-allowoverrides-security-bypass(50808)

Vulnerability Solution:

Apache >= 2.2 and < 2.2.12
Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.26. Apache HTTPD: expat DoS (CVE-2009-3560) (apache-httpd-cve-2009-3560)

Description:

The affected asset is vulnerable to this vulnerability ONLY if an attacker is able to get Apache to parse an untrusted XML document. Review your Web server configuration for validation.The affected asset is vulnerable to this vulnerability ONLY if an attacker is able to get Apache to parse an untrusted XML document. Review your Web server configuration for validation.A buffer over-read flaw was found in the bundled expat library. An attacker who is able to get Apache to parse an untrused XML document (for example through mod_dav) may be able to cause a crash. This crash would only be a denial of service if using the worker MPM.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	37203
CVE	CVE-2009-3560
DEBIAN	DSA-1953
IAVM	2012-A-0020
OVAL	OVAL10613
OVAL	OVAL12942
OVAL	OVAL6883
REDHAT	RHSA-2011:0896
SECUNIA	37537
SECUNIA	38231
SECUNIA	38794
SECUNIA	38832
SECUNIA	38834

Source	Reference
SECUNIA	39478
SECUNIA	41701
SECUNIA	43300
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache >= 2.2 and < 2.2.17

Upgrade to Apache HTTPD version 2.2.17

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.27. Apache HTTPD: expat DoS (CVE-2009-3720) (apache-httpd-cve-2009-3720)

Description:

The affected asset is vulnerable to this vulnerability ONLY if an attacker is able to get Apache to parse an untrusted XML document. Review your Web server configuration for validation.The affected asset is vulnerable to this vulnerability ONLY if an attacker is able to get Apache to parse an untrusted XML document. Review your Web server configuration for validation.A buffer over-read flaw was found in the bundled expat library. An attacker who is able to get Apache to parse an untrused XML document (for example through mod_dav) may be able to cause a crash. This crash would only be a denial of service if using the worker MPM.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
CVE	CVE-2009-3720
IAVM	2012-A-0020
OVAL	OVAL11019
OVAL	OVAL12719

Source	Reference
OVAL	OVAL7112
REDHAT	RHSA-2010:0002
REDHAT	RHSA-2011:0896
SECUNIA	37324
SECUNIA	37537
SECUNIA	37925
SECUNIA	38050
SECUNIA	38231
SECUNIA	38794
SECUNIA	38832
SECUNIA	38834
SECUNIA	39478
SECUNIA	41701
SECUNIA	42326
SECUNIA	42338
SECUNIA	43300
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache >= 2.2 and < 2.2.17

Upgrade to Apache HTTPD version 2.2.17

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.28. Apache HTTPD: mod_proxy_ajp DoS (CVE-2010-0408) (apache-httpd-cve-2010-0408)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running module mod_proxy_ajp. Review your Web server configuration for validation.mod_proxy_ajp would return the wrong status code if it encountered an error, causing a backend server to be put into an error state until the retry timeout expired. A remote attacker could send malicious requests to trigger this issue, resulting in denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2010-11-10-1
BID	38491
CVE	CVE-2010-0408
DEBIAN	DSA-2035
OVAL	OVAL8619
OVAL	OVAL9935
REDHAT	RHSA-2010:0168
SECUNIA	39100
SECUNIA	39501
SECUNIA	39628
SECUNIA	39632
SECUNIA	39656
SECUNIA	40096
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.2 and < 2.2.15

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.29. Apache HTTPD: mod_dav DoS (CVE-2010-1452) (apache-httpd-cve-2010-1452)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running module mod_cache or mod_dav. Review your Web server configuration for validation.A flaw was found in the handling of requests by mod_dav. A malicious remote attacker could send a carefully crafted request and cause a httpd child process to crash. This crash would only be a denial of service if using the worker MPM. This issue is further mitigated as mod_dav is only affected by requests that are most likely to be authenticated.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
CVE	CVE-2010-1452
IAVM	2012-B-0056
OVAL	OVAL11683
OVAL	OVAL12341
REDHAT	RHSA-2010:0659
REDHAT	RHSA-2011:0896
REDHAT	RHSA-2011:0897
SECUNIA	42367
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache >= 2.2 and < 2.2.16

Upgrade to Apache HTTPD version 2.2.16

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.16.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.30. Apache HTTPD: apr_bridage_split_line DoS (CVE-2010-1623) (apache-httpd-cve-2010-1623)

Description:

The affected asset is vulnerable to this vulnerability ONLY if if Apache processes non-SSL requests. Review your Web server configuration for validation.The affected asset is vulnerable to this vulnerability ONLY if if Apache processes non-SSL requests. Review your Web server configuration for validation.A flaw was found in the apr_brigade_split_line() function of the bundled APR-util library, used to process non-SSL requests. A remote attacker could send requests, carefully crafting the timing of individual bytes, which would slowly consume memory, potentially leading to a denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	43673
CVE	CVE-2010-1623
IAVM	2012-B-0056
OVAL	OVAL12800
REDHAT	RHSA-2010:0950
REDHAT	RHSA-2011:0896
REDHAT	RHSA-2011:0897
SECUNIA	41701
SECUNIA	42015
SECUNIA	42361
SECUNIA	42367
SECUNIA	42403
SECUNIA	42537
SECUNIA	43211
SECUNIA	43285
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache >= 2.2 and < 2.2.17

Upgrade to Apache HTTPD version 2.2.17

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.31. Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368) (apache-httpd-cve-2011-3368)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running module mod_proxy. Review your Web server configuration for validation.An exposure was found when using mod_proxy in reverse proxy mode. In certain configurations using RewriteRule with proxy flag, a remote attacker could cause the reverse proxy to connect to an arbitrary server, possibly disclosing sensitive information from internal web servers not directly accessible to attacker. No update of 1.3 will be released. Patches will be published to http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	49957
CVE	CVE-2011-3368
IAVM	2012-A-0017
IAVM	2012-B-0056
OSVDB	76079
REDHAT	RHSA-2011:1391
REDHAT	RHSA-2011:1392
SECUNIA	46288
SECUNIA	46414
URL	http://httpd.apache.org/security/vulnerabilities_13.html
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html
XF	apache-modproxy-information-disclosure(70336)

Vulnerability Solution:

•Apache >= 1.3 and < 2

Apply the patch for CVE-2011-3368 to 1.3

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/
No update of 1.3 will be released. Patches will be published to http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/

•Apache >= 2.0 and < 2.0.65

Upgrade to Apache HTTPD version 2.0.65

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache >= 2.2 and < 2.2.22

Upgrade to Apache HTTPD version 2.2.22

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.32. Apache HTTPD: scoreboard parent DoS (CVE-2012-0031) (apache-httpd-cve-2012-0031)

Description:

A flaw was found in the handling of the scoreboard. An unprivileged child process could cause the parent process to crash at shutdown rather than terminate cleanly.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	51407
CVE	CVE-2012-0031
IAVM	2012-A-0017
REDHAT	RHSA-2012:0128
SECUNIA	47410
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.2 and < 2.2.22
Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.33. Anonymous users can obtain the Windows password policy (cifs-nt-0002)

Description:

Anonymous users can obtain the Windows password policy from the system by using CIFS NULL sessions. The password policy contains sensitive information about minimum password length, password lockout threshold, password lockout duration, etc.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3	Retrieved domain policy for the METASPLOITABLE domain, with SID S-1-5-21-1042354039-2475377354-766472396

References:

Source	Reference
BID	959
CVE	CVE-2000-1200
XF	nt-lsa-domain-sid(4015)

Vulnerability Solution:

- Microsoft Windows 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003, Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003

Disable NULL sessions

Modify the registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\
```

with the following values:

```
     Value Name: RestrictAnonymous
     Data Type: REG_DWORD
     Data Value: 1

     Value Name: RestrictAnonymousSAM
     Data Type: REG_DWORD
     Data Value: 1

     Value Name: EveryoneIncludesAnonymous
     Data Type: REG_DWORD
     Data Value: 0
```

and set the following value to 0 (or, alternatively, delete it):

```
     Value Name: TurnOffAnonymousBlock
     Data Type: REG_DWORD
     Data Value: 0
```

Modify the registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\
```

with the following values:

```
     Value Name: RestrictNullSessAccess
     Data Type: REG_DWORD
     Data Value: 1
```

```
      Value Name: NullSessionPipes
      Data Type: REG_MULTI_SZ
      Data Value: "" (empty string, without quotes)
```

Open Local Security Settings, and disable the following setting:

```
       Security Settings -> Local Policies -> Security Options ->
       Network access: Allow anonymous SID/Name translation: Disabled
```

Finally, reboot the machine.

Please note that disabling NULL sessions may have an adverse impact on functionality, as some applications and network environments may depend on them for proper operation. Refer to Microsoft Knowledge Base Article 823659 for more information.

- Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional

Disable NULL sessions

Modify the registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\
```

with the following values:

```
      Value Name: RestrictAnonymous
      Data Type: REG_DWORD
      Data Value: 1

      Value Name: RestrictAnonymousSAM
      Data Type: REG_DWORD
      Data Value: 1

      Value Name: EveryoneIncludesAnonymous
      Data Type: REG_DWORD
      Data Value: 0
```

Modify the registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\
```

with the following values:

```
      Value Name: RestrictNullSessAccess
      Data Type: REG_DWORD
      Data Value: 1

      Value Name: NullSessionPipes
      Data Type: REG_MULTI_SZ
      Data Value: "" (empty string, without quotes)
```

Open Local Security Settings, and disable the following setting:

```
       Security Settings -> Local Policies -> Security Options ->
       Network access: Allow anonymous SID/Name translation: Disabled
```

Finally, reboot the machine.

Please note that disabling NULL sessions may have an adverse impact on functionality, as some applications and network environments may depend on them for proper operation. Refer to Microsoft Knowledge Base Article Q246261 for more information.

- Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server

Disable NULL sessions

Modify the registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\
```

with the following value:

```
Value Name: RestrictAnonymous
Data Type: REG_DWORD
Data Value: 2
```

After modifying the registry, reboot the machine.

Please note that disabling NULL sessions may have an adverse impact on functionality, as some applications and network environments may depend on them for proper operation. Refer to Microsoft Knowledge Base Article Q246261 for more information.

- Microsoft Windows NT Server 4.0, Microsoft Windows NT Server, Enterprise Edition 4.0, Microsoft Windows NT Workstation 4.0

Install Microsoft service pack Windows NT4 Service Pack 4

Download and apply the upgrade from: http://support.microsoft.com/sp

- Microsoft Windows NT, Microsoft Windows NT Workstation, Microsoft Windows NT Server, Microsoft Windows NT Advanced Server, Microsoft Windows NT Server, Enterprise Edition, Microsoft Windows NT Server, Terminal Server Edition

Disable NULL sessions

Modify the registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\
```

with the following value:

```
Value Name: RestrictAnonymous
Data Type: REG_DWORD
Data Value: 1
```

After modifying the registry, reboot the machine.

It is important to note that on Windows NT 4.0 systems, setting this registry entry will still leave the system open to various attacks, including brute-force enumeration of users and groups. A complete solution for Windows NT 4.0 systems is not available.

- Samba on Linux

Restrict anonymous access

To restrict anonymous access to Samba, modify your "smb.conf" settings as follows:

```
                   guest account = nobody
                   restrict anonymous = 1

Note: Make sure you do NOT list a user "nobody" in your password file.
```

- Novell NetWare

Novell Netware CIFS

As of May 9, 2007 Novell Netware CIFS does not provide a workaround for this vulnerability.

3.2.34. Samba Connection Flooding Denial of Service Vulnerability (cifs-samba-connection-flooding-dos)

Description:

Certain versions of Samba are vulnerable to a denial of service condition when handling multiple incoming connection requests. Successful exploitation allows an unauthenticated attacker to exhaust all available memory on the target system, causing the daemon to hang.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:139	Running vulnerable CIFS service: Samba 3.0.20-Debian.
192.168.56.3:445	Running vulnerable CIFS service: Samba 3.0.20-Debian.

References:

Source	Reference
APPLE	APPLE-SA-2006-11-28
BID	18927
CERT	TA06-333A
CERT-VN	313836
CVE	CVE-2006-3403
DEBIAN	DSA-1110
OVAL	OVAL11355
REDHAT	RHSA-2006:0591
SECUNIA	20980
SECUNIA	20983
SECUNIA	21018
SECUNIA	21019
SECUNIA	21046
SECUNIA	21086
SECUNIA	21143
SECUNIA	21159
SECUNIA	21187
SECUNIA	21190
SECUNIA	21262

Source	Reference
SECUNIA	22875
SECUNIA	23155
SGI	20060703-01-P
URL	http://samba.org/samba/security/CVE-2006-3403.html
XF	samba-smbd-connection-dos(27648)

Vulnerability Solution:

Download and apply the upgrade from: http://us1.samba.org/samba/ftp/old-versions/samba-3.0.23.tar.gz

3.2.35. Database Open Access (database-open-access)

Description:

The database allows any remote system the ability to connect to it. It is recommended to limit direct access to trusted systems because databases may contain sensitive data, and new vulnerabilities and exploits are discovered routinely for them. For this reason, it is a violation of PCI DSS section 1.3.7 to have databases listening on ports accessible from the Internet, even when protected with secure authentication mechanisms.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:3306	Running vulnerable MySQL service.
192.168.56.3:5432	Running vulnerable Postgres service.

References:

Source	Reference
URL	https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-2.pdf

Vulnerability Solution:

Configure the database server to only allow access to trusted systems. For example, the PCI DSS standard requires you to place the database in an internal network zone, segregated from the DMZ

3.2.36. BIND 9 Resolver crashes after logging an error in query.c (dns-bind-cve-2011-4313)

Description:

An as-yet unidentified network event caused BIND 9 resolvers to cache an invalid record, subsequent queries for which could crash the resolvers with an assertion failure. ISC is working on determining the ultimate cause by which a record with this particular inconsistency is cached.At this time we are making available a patch which makes named recover gracefully from the inconsistency, preventing the abnormal exit.

The patch has two components. When a client query is handled, the code which processes the response to the client has to ask the cache for the records for the name that is being queried. The first component of the patch prevents the cache from returning the inconsistent data. The second component prevents named from crashing if it detects that it has been given an inconsistent answer of this nature.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:53	Running vulnerable DNS service: BIND 9.4.2.

References:

Source	Reference
BID	50690
CERT-VN	606539
CVE	CVE-2011-4313
DEBIAN	DSA-2347
OSVDB	77159
REDHAT	RHSA-2011:1458
REDHAT	RHSA-2011:1459
REDHAT	RHSA-2011:1496
SECUNIA	46536
SECUNIA	46829
SECUNIA	46887
SECUNIA	46890
SECUNIA	46905
SECUNIA	46906
SECUNIA	46943
SECUNIA	46984
SECUNIA	47043
SECUNIA	47075
XF	isc-bind-recursive-dos(71332)

Vulnerability Solution:

•Apply patch to mitigate BIND 9 resolver crash

Patches mitigating this issue are available at:

•https://www.isc.org/software/bind/981-p1

•https://www.isc.org/software/bind/974-p1

•https://www.isc.org/software/bind/96-esv-r5-p1

•https://www.isc.org/software/bind/94-esv-r5-p1

•Upgrade to BIND version 9.4-ESV-R5-P1

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.4-ESV-R5-P1/bind-9.4-ESV-R5-P1.tar.gz

Upgrade to 9.4-ESV-R5-P1 version of ISC BIND Which was released on November 16, 2011. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.6-ESV-R5-P1

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.6-ESV-R5-P1/bind-9.6-ESV-R5-P1.tar.gz
Upgrade to 9.6-ESV-R5-P1 version of ISC BIND Which was released on November 16, 2011. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.7.4-P1

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.7.4-P1/bind-9.7.4-P1.tar.gz
Upgrade to 9.7.4-P1 version of ISC BIND Which was released on November 16, 2011. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.8.1-P1

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.8.1-P1/bind-9.8.1-P1.tar.gz
Upgrade to 9.8.1-P1 version of ISC BIND Which was released on November 16, 2011. The source code and binaries for this release can be downloaded from bind's website.

3.2.37. BIND: Ghost Domain Names: Revoked Yet Still Resolvable (dns-bind-cve-2012-1033)

Description:

The resolver in ISC BIND 9 through 9.8.1-P1 does not properly implement a cache update policy, which allows remote attackers to trigger continued resolvability of domain names that are no longer registered via an unspecified "Ghost Names exploit."

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:53	Running vulnerable DNS service: BIND 9.4.2.

References:

Source	Reference
BID	51898
CERT-VN	542123
CVE	CVE-2012-1033
OSVDB	78916
SECUNIA	47884
XF	isc-bind-update-sec-bypass(73053)

Vulnerability Solution:

If you are aware that you have cached bad records, clearing the cache will remove them but is not an effective or practical preventative approach.

3.2.38. ISC BIND DNSSEC EVP_VerifyFinal() and DSA_do_verify() Spoofing Vulnerability (dns-bind-ssl-signature-spoofing)

Description:

OpenSSL security advisory CVE-2008-5077 may affect BIND users. The OpenSSL advisory says Several functions inside OpenSSL incorrectly checked the result after calling the EVP_VerifyFinal function, allowing a malformed signature to be treated as a good signature rather than as an error. This issue affected the signature checks on DSA and ECDSA keys used with SSL/TLS. It is theoretically possible to spoof answers returned from zones whose DNSKEY algorithms are affected by that OpenSSL issue.

Affected Nodes:

Affected Nodes:	**Additional Information:**
192.168.56.3:53	Running vulnerable DNS service: BIND 9.4.2.

References:

Source	**Reference**
APPLE	APPLE-SA-2009-05-12
CERT	TA09-133A
CVE	CVE-2009-0025
OVAL	OVAL10879
OVAL	OVAL5569
SECUNIA	33494
SECUNIA	33546
SECUNIA	33551
SECUNIA	33559
SECUNIA	33683
SECUNIA	33882
SECUNIA	35074
URL	https://www.isc.org/node/389

Vulnerability Solution:

•Upgrade to BIND version 9.3.6-P1

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.3.6-P1/bind-9.3.6-P1.tar.gz
Upgrade to 9.3.6-P1 version of ISC BIND Which was released on January 07, 2009. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.4.3-P1

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.4.3-P1/bind-9.4.3-P1.tar.gz
Upgrade to 9.4.3-P1 version of ISC BIND Which was released on January 07, 2009. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.5.1-P1

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.5.1-P1/bind-9.5.1-P1.tar.gz
Upgrade to 9.5.1-P1 version of ISC BIND Which was released on January 07, 2009. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.6.0-P1

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.6.0-P1/bind-9.6.0-P1.tar.gz
Upgrade to 9.6.0-P1 version of ISC BIND Which was released on January 07, 2009. The source code and binaries for this release can be downloaded from bind's website.

3.2.39. Debian Linux httpd Vulnerability (http-apache-0007)

Description:

The Debian GNU/Linux 2.1 Apache package by default allows anyone to view /usr/doc via the web, remotely. This is because srm.conf is preconfigured with the line:

Alias /doc/ /usr/doc/

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8. http://192.168.56.3/doc/ 4: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"> 5: <html> 6: <head> 4: <title>Index of /doc</title>

References:

Source	Reference
BID	318
CVE	CVE-1999-0678
URL	http://www.netspace.org/cgi-bin/wa?A2=ind9904a&L=bugtraq&F=&S=&P=2822

Vulnerability Solution:

The following addition to /etc/apache/access.conf will restrict access:

```
 <Directory /usr/doc>
AllowOverride None order deny,allow
deny from all
allow from localhost
</Directory>
```

3.2.40. WebDAV Extensions are Enabled (http-generic-webdav-enabled)

Description:

WebDAV is a set of extensions to the HTTP protocol that allows users to collaboratively edit and manage files on remote web servers. Many web servers enable WebDAV extensions by default, even when they are not needed. Because of its added complexity, it is considered good practice to disable WebDAV if it is not currently in use.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

None

Vulnerability Solution:

•IIS, PWS, Microsoft-IIS, Internet Information Services, Internet Information Services, Microsoft-PWS

Disable WebDAV for IIS

For Microsoft IIS, follow Microsoft's instructions to disable WebDAV for the entire server.

•Apache

Disable WebDAV for Apache

Make sure the mod_dav module is disabled, or ensure that authentication is required on directories where DAV is required.

•Apache Tomcat, Tomcat, Tomcat Web Server

Disable WebDAV for Apache Tomcat

Disable the WebDAV Servlet for all web applications found on the web server. This can be done by removing the servlet definition for WebDAV (the org.apache.catalina.servlets.WebdavServlet class) and remove all servlet mappings referring to the WebDAV servlet.

•Java System Web Server, iPlanet, SunONE WebServer, Sun-ONE-Web-Server

Disable WebDAV for iPlanet/Sun ONE

Disable WebDAV on the web server. This can be done by disabling WebDAV for the server instance and for all virtual servers.

To disable WebDAV for the server instance, enter the Server Manager and uncheck the "Enable WebDAV Globally" checkbox then click the "OK" button.

To disable WebDAV for each virtual server, enter the Class Manager and uncheck the "Enable WebDAV Globally" checkbox next to each server instance then click the "OK" button.

3.2.41. PHP 5.2.5 cURL safe_mode bypass (http-php-curl-safe-mode-bypass-other)

Description:

Certain versions of PHP contain a weakness whereby calls to the cURL extension can bypass Safe Mode restrictions. As a result, a script can be constructed to access files it did not normally have permission to manipulate.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2008-07-31
APPLE	APPLE-SA-2008-10-09
BID	27413
BID	29009
BID	31681
CVE	CVE-2007-4850
SECUNIA	30048
SECUNIA	30411
SECUNIA	31200
SECUNIA	31326
SECUNIA	32222
URL	http://article.gmane.org/gmane.comp.security.full-disclosure/58593
URL	http://www.php.net/releases/5_2_6.php
XF	php-curlinit-security-bypass(39852)
XF	php-safemode-directive-security-bypass(42134)

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.6.tar.gz
Upgrade to PHP v5.2.6.

3.2.42. PHP Multiple Vulnerabilities Fixed in version 5.2.9 (http-php-multiple-vulns-5-2-9)

Description:

Certain versions of PHP ship with a vulnerable version of the imageRotate function. This could allow a context-dependent attacker to read the contents of arbitrary memory via a specially crafted value of the third argument for an indexed image. (CVE-2008-5498)

An unspecified error in the zip functionality could cause a crash when file or directory names contain a relative path (CVE-2009-1272)

An unspecified error exists in the explode() function.

An unspecified error exists when a malformed string is passed to the json_decode() function (CVE-2009-1271)

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2009-09-10-2
CVE	CVE-2009-1271
CVE	CVE-2009-1272
DEBIAN	DSA-1775
DEBIAN	DSA-1789
REDHAT	RHSA-2009:0350
SECUNIA	34770
SECUNIA	34830
SECUNIA	34933
SECUNIA	35003
SECUNIA	35007
SECUNIA	35306
SECUNIA	35685
SECUNIA	36701
URL	http://www.php.net/ChangeLog-5.php#5.2.9
URL	http://www.php.net/releases/5_2_9.php

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.9.tar.gz
Upgrade to PHP v5.2.9.

3.2.43. PHP Multiple Vulnerabilities Fixed in version 5.3.2 (http-php-multiple-vulns-5-3-2)

Description:

Improved LCG entropy.

Fixed safe_mode validation inside tempnam() when the directory path does not end with a /.

Fixed a possible open_basedir/safe_mode bypass in the session extension identified by Grzegorz Stachowiak.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
URL	http://www.php.net/ChangeLog-5.php#5.3.2
URL	http://www.php.net/releases/5_3_2.php

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.3.2.tar.gz/from/a/mirror
Upgrade to PHP v5.3.2 (released on March 4th, 2010).

3.2.44. PHP IMAP toolkit crash: rfc822.c legacy routine buffer overflow (http-php-rfc822-write-address-bof)

Description:

php_imap.c in PHP 5.2.5, 5.2.6, 4.x, and other versions, uses obsolete API calls that allow context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long IMAP request, which triggers an "rfc822.c legacy routine buffer overflow" error message, related to the rfc822_write_address function.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2009-05-12
BID	29829
CERT	TA09-133A
CVE	CVE-2008-2829
OSVDB	46641
SECUNIA	31200
SECUNIA	35074
SECUNIA	35306
SECUNIA	35650
XF	php-phpimap-dos(43357)

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.7.tar.gz
Upgrade to PHP v5.2.7.

3.2.45. PHP Fixed security issues (CVE-2008-2665) (http-php-safemode-bypass3)

Description:

Directory traversal vulnerability in the posix_access function in PHP 5.2.6 and earlier allows remote attackers to bypass safe_mode restrictions via a .. (dot dot) in an http URL, which results in the URL being canonicalized to a local filename after the safe_mode check has successfully run.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2009-05-12
BID	29797
CERT	TA09-133A
CVE	CVE-2008-2665
SECUNIA	35074
SECUNIA	35650
XF	php-posixaccess-security-bypass(43196)

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.7.tar.gz
Upgrade to PHP v5.2.7.

3.2.46. MySQL 'DATA DIRECTORY' and 'INDEX DIRECTORY' MyISAM Table Privilege Escalation Vulnerability (mysql-datadir-isam-table-privilege-escalation)

Description:

MySQL 4.1.x before 4.1.24, 5.0.x before 5.0.60, 5.1.x before 5.1.24, and 6.0.x before 6.0.5 allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are within the MySQL home data directory, which can point to tables that are created in the future.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:3306	Running vulnerable MySQL service: MySQL 5.0.51a.

References:

Source	Reference
APPLE	APPLE-SA-2008-10-09
APPLE	APPLE-SA-2009-09-10-2
BID	29106
BID	31681
CVE	CVE-2008-2079
DEBIAN	DSA-1608
OVAL	OVAL10133
REDHAT	RHSA-2008:0505

Source	Reference
REDHAT	RHSA-2008:0510
REDHAT	RHSA-2008:0768
SECUNIA	30134
SECUNIA	31066
SECUNIA	31226
SECUNIA	31687
SECUNIA	32222
SECUNIA	36701
URL	http://bugs.mysql.com/32091
URL	http://dev.mysql.com/doc/refman/5.1/en/news-5-1-23.html
URL	http://dev.mysql.com/doc/refman/6.0/en/news-6-0-4.html
XF	mysql-myisam-security-bypass(42267)

Vulnerability Solution:

•MySQL (?:^4.1.)

Upgrade to MySQL v4.1.24

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/4.1.html

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•MySQL >= 5.0.0 and < 5.0.60

Upgrade to MySQL v5.0.60

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.0.html

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•MySQL (?:^5.1.)

Upgrade to MySQL v5.1.24

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.1.html

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•MySQL (?:^6.0.)

Upgrade to MySQL v6.0.5

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/6.0.html

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.47. MySQL my_net_skip_rest Packet Length Denial of Service Vulnerability (mysql-my_net_skip_rest-packet-length-dos)

Description:

The my_net_skip_rest function in sql/net_serv.cc in MySQL 5.0 before 5.0.91 and 5.1 before 5.1.47 allows remote attackers to cause a denial of service (CPU and bandwidth consumption) by sending a large number of packets that exceed the maximum length.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:3306	Running vulnerable MySQL service: MySQL 5.0.51a.

References:

Source	Reference
APPLE	APPLE-SA-2010-11-10-1
CVE	CVE-2010-1849
OVAL	OVAL7328
URL	http://bugs.mysql.com/bug.php?id=50974
URL	http://bugs.mysql.com/bug.php?id=53371
URL	http://dev.mysql.com/doc/refman/5.1/en/news-5-1-47.html

Vulnerability Solution:

•MySQL >= 5.0.0 and < 5.0.91

Upgrade to MySQL v5.0.91

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.0.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•MySQL >= 5.1.0 and < 5.1.47

Upgrade to MySQL v5.1.47

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.1.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.48. MySQL MyISAM Table Privilege Check Bypass (mysql-myisam-table-privilege-check-bypass)

Description:

Certain versions of MySQL allow local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified DATA DIRECTORY or INDEX DIRECTORY arguments that are originally associated with pathnames without symlinks, and that can point to tables created at a future time at which a pathname is modified to contain a symlink to a subdirectory of the MySQL home data directory.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.56.3:3306	Running vulnerable MySQL service: MySQL 5.0.51a.

References:

Source	Reference
CVE	CVE-2008-4097
CVE	CVE-2008-4098
OVAL	OVAL10591
REDHAT	RHSA-2009:1067
REDHAT	RHSA-2010:0110
SECUNIA	32759
SECUNIA	38517
URL	http://bugs.mysql.com/bug.php?id=32167
URL	http://lists.mysql.com/commits/50036
URL	http://lists.mysql.com/commits/50773
XF	mysql-myisam-symlink-security-bypass(45649)
XF	mysql-myisam-symlinks-security-bypass(45648)

Vulnerability Solution:

•MySQL >= 6.0.0 and < 6.0.10

Upgrade to MySQL v6.0.10

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/6.0.html

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•MySQL >= 5.1.0 and < 5.1.32

Upgrade to MySQL v5.1.32

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.1.html

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•MySQL >= 5.0.0 and < 5.0.68

Upgrade to MySQL v5.0.77

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.0.html

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•MySQL (?:^4.1.)

Upgrade to MySQL v4.1.25

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/4.1.html

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.49. Exported volume is publicly mountable (nfs-mountd-0002)

Description:

An NFS volume is mountable by everyone. Although this is not necessarily a vulnerability itself, this does not exhibit "best practice" from a security standpoint; mounting privileges should be restricted only to hosts that require them.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:33649	/
192.168.56.3:37000	/

References:

None

Vulnerability Solution:

Restrict mounting privileges to only hosts that require them.

3.2.50. PHP Crash with URI/file..php (php-crash-with-uri-file-php)

Description:

PHP 4.4.x before 4.4.9, and 5.x through 5.2.6, when used as a FastCGI module, allows remote attackers to cause a denial of service (crash) via a request with multiple dots preceding the extension, as demonstrated using foo..php.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2009-05-12
CERT	TA09-133A
CVE	CVE-2008-3660
DEBIAN	DSA-1647
OVAL	OVAL9597
REDHAT	RHSA-2009:0350
SECUNIA	31982
SECUNIA	32148
SECUNIA	35074
SECUNIA	35306
SECUNIA	35650

Source	Reference
XF	php-curl-unspecified(44402)

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.7.tar.gz
Upgrade to PHP v5.2.7.

3.2.51. PHP PHP hangs on numeric value 2.2250738585072011e-308 (php-cve-2010-4645)

Description:

strtod.c, as used in the zend_strtod function in PHP 5.2 before 5.2.17 and 5.3 before 5.3.5, and other products, allows context-dependent attackers to cause a denial of service (infinite loop) via a certain floating-point value in scientific notation, which is not properly handled in x87 FPU registers, as demonstrated using 2.2250738585072011e-308.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
BID	45668
CVE	CVE-2010-4645
IAVM	2012-B-0056
REDHAT	RHSA-2011:0195
REDHAT	RHSA-2011:0196
SECUNIA	42812
SECUNIA	42843
SECUNIA	43051
SECUNIA	43189
XF	php-zendstrtod-dos(64470)

Vulnerability Solution:

- Upgrade to PHP v5.2.17

  Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.17.tar.gz
  Upgrade to PHP v5.2.17.

- Upgrade to PHP v5.3.5

  Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.5.tar.gz
  Upgrade to PHP v5.3.5.

3.2.52. PHP multiple NULL Pointer Dereference with zend_strndup()) (php-cve-2011-4153)

Description:

PHP 5.3.8 does not always check the return value of the zend_strndup function, which might allow remote attackers to cause a denial of service (NULL pointer dereference and application crash) via crafted input to an application that performs strndup operations on untrusted string data, as demonstrated by the define function in zend_builtin_functions.c, and unspecified functions in ext/soap/php_sdl.c, ext/standard/syslog.c, ext/standard/browscap.c, ext/oci8/oci8.c, ext/com_dotnet/com_typeinfo.c, and main/php_open_temporary_file.c.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
CVE	CVE-2011-4153
SECUNIA	48668

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.4.0.tar.gz
Upgrade to PHP v5.4.0.

3.2.53. PHP Fixed bug #61807 Buffer Overflow in apache_request_headers (php-cve-2012-2329)

Description:

Buffer overflow in the apache_request_headers function in sapi/cgi/cgi_main.c in PHP 5.4.x before 5.4.3 allows remote attackers to cause a denial of service (application crash) via a long string in the header of an HTTP request.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	53455
CVE	CVE-2012-2329
SECUNIA	49014
XF	php-apacherequestheaders-bo(75545)

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.4.3.tar.gz
Upgrade to PHP v5.4.3.

3.2.54. PHP Fixed iconv_*() functions to limit argument sizes (CVE-2007-4783) (php-fixed-iconv-functions-to-limit-argument-sizes-cve-2007-4783)

Description:

The iconv_substr function in PHP 5.2.4 and earlier allows context-dependent attackers to cause (1) a denial of service (application crash) via a long string in the charset parameter, probably also requiring a long string in the str parameter; or (2) a denial of service (temporary application hang) via a long string in the str parameter. NOTE: this might not be a vulnerability in most web server environments that support multiple threads, unless these issues can be demonstrated for code execution.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
CVE	CVE-2007-4783
OSVDB	38917
SECUNIA	27102
SECUNIA	27659
SECUNIA	30040

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.5.tar.gz
Upgrade to PHP v5.2.5.

3.2.55. PHP Fixed iconv_*() functions to limit argument sizes (CVE-2007-4840) (php-fixed-iconv-functions-to-limit-argument-sizes-cve-2007-4840)

Description:

PHP 5.2.4 and earlier allows context-dependent attackers to cause a denial of service (application crash) via (1) a long string in the out_charset parameter to the iconv function; or a long string in the charset parameter to the (2) iconv_mime_decode_headers, (3) iconv_mime_decode, or (4) iconv_strlen function. NOTE: this might not be a vulnerability in most web server environments that support multiple threads, unless these issues can be demonstrated for code execution.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
CVE	CVE-2007-4840
OSVDB	38916
SECUNIA	27102
SECUNIA	27659
SECUNIA	28658
SECUNIA	30040
SUSE	SUSE-SA:2008:004

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.5.tar.gz
Upgrade to PHP v5.2.5.

3.2.56. PHP Fixed possible flaw in open_basedir (php-fixed-possible-flaw-in-open-basedir)

Description:

fopen_wrappers.c in PHP 5.3.x through 5.3.3 might allow remote attackers to bypass open_basedir restrictions via vectors related to the length of a filename.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
APPLE	APPLE-SA-2011-10-12-3
BID	44723
CVE	CVE-2010-3436
IAVM	2012-B-0056
SECUNIA	42729
SECUNIA	42812

Vulnerability Solution:

•Upgrade to PHP v5.2.15

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.15.tar.gz
Upgrade to PHP v5.2.15.

•Upgrade to PHP v5.3.4

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz

Upgrade to PHP v5.3.4.

3.2.57. PHP Fixed security issue in imagerotate() (php-fixed-security-issue-in-imagerotate)

Description:

Array index error in the imageRotate function in PHP 5.2.8 and earlier allows context-dependent attackers to read the contents of arbitrary memory locations via a crafted value of the third argument (aka the bgd_color or clrBack argument) for an indexed image.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2009-09-10-2
BID	33002
CVE	CVE-2008-5498
OSVDB	51031
OVAL	OVAL9667
REDHAT	RHSA-2009:0350
SECUNIA	34642
SECUNIA	35306
SECUNIA	35650
SECUNIA	36701
XF	php-imagerotate-info-disclosure(47635)

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.9.tar.gz
Upgrade to PHP v5.2.9.

3.2.58. PHP Fixed security issues (CVE-2008-2666) (php-fixed-security-issues-cve-2008-2666)

Description:

Multiple directory traversal vulnerabilities in PHP 5.2.6 and earlier allow context-dependent attackers to bypass safe_mode restrictions by creating a subdirectory named http: and then placing ../ (dot dot slash) sequences in an http URL argument to the (1) chdir or (2) ftok function.

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2009-05-12
BID	29796
CERT	TA09-133A
CVE	CVE-2008-2666
SECUNIA	35074
SECUNIA	35650
XF	php-chdir-ftoc-security-bypass(43198)

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.7.tar.gz
Upgrade to PHP v5.2.7.

3.2.59. PHP NULL pointer dereference when processing invalid XML-RPC requests (php-null-pointer-dereference-when-processing-invalid-xml-rpc-requests)

Description:

The xmlrpc extension in PHP 5.3.1 does not properly handle a missing methodName element in the first argument to the xmlrpc_decode_request function, which allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) and possibly have unspecified other impact via a crafted argument.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2010-08-24-1
APPLE	APPLE-SA-2010-11-10-1
BID	38708
CVE	CVE-2010-0397
REDHAT	RHSA-2010:0919
SECUNIA	42410

Vulnerability Solution:

•Upgrade to PHP v5.2.14

Download and apply the upgrade from: http://www.php.net/get/php-5.2.14.tar.gz/from/a/mirror

Upgrade to PHP v5.2.14.

•Upgrade to PHP v5.3.3

Download and apply the upgrade from: http://www.php.net/get/php-5.3.3.tar.gz/from/a/mirror
Upgrade to PHP v5.3.3.

3.2.60. PHP possible double free in imap extension (php-possible-double-free-in-imap-extension)

Description:

Double free vulnerability in the imap_do_open function in the IMAP extension (ext/imap/php_imap.c) in PHP 5.2 before 5.2.15 and 5.3 before 5.3.4 allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
BID	44980
CVE	CVE-2010-4150
OVAL	OVAL12489
SECUNIA	42729
XF	php-phpimapc-dos(63390)

Vulnerability Solution:

•Upgrade to PHP v5.2.15

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.15.tar.gz
Upgrade to PHP v5.2.15.

•Upgrade to PHP v5.3.4

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz
Upgrade to PHP v5.3.4.

3.2.61. PHP possible interruption array leak in strrchr() (php-possible-interruption-array-leak-in-strrchr)

Description:

The strrchr function in PHP 5.2 before 5.2.14 allows context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal function or handler.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2010-08-24-1
APPLE	APPLE-SA-2010-11-10-1
CVE	CVE-2010-2484

Vulnerability Solution:

Download and apply the upgrade from: http://www.php.net/get/php-5.2.14.tar.gz/from/a/mirror
Upgrade to PHP v5.2.14.

3.2.62. TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)

Description:

TCP, when using a large Window Size, makes it easier for remote attackers to guess sequence numbers and cause a denial of service (connection loss) to persistent TCP connections by repeatedly injecting a TCP RST packet, especially in protocols that use long-lived connections, such as BGP.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3	TCP reset with incorrect sequence number triggered this fault on 192.168.56.3:512: Connection reset by peer

References:

Source	Reference
BID	10183
CERT	TA04-111A
CERT-VN	415294
CVE	CVE-2004-0230
MS	MS05-019
MS	MS06-064
NETBSD	NetBSD-SA2004-006
OSVDB	4030
OVAL	OVAL2689
OVAL	OVAL270

Source	Reference
OVAL	OVAL3508
OVAL	OVAL4791
OVAL	OVAL5711
SECUNIA	11440
SECUNIA	11458
SECUNIA	22341
SGI	20040403-01-A
URL	ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc
URL	http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12
URL	http://www.uniras.gov.uk/vuls/2004/236929/index.htm
XF	tcp-rst-dos(15886)

Vulnerability Solution:

•Microsoft Windows Server 2003, Web Edition < SP1, Microsoft Windows Server 2003, Enterprise Edition < SP1, Microsoft Windows Server 2003, Datacenter Edition < SP1, Microsoft Windows Server 2003, Standard Edition < SP1, Microsoft Windows Small Business Server 2003 < SP1

Download and install Microsoft patch WindowsServer2003-KB893066-v2-x86-enu.EXE

Download and apply the patch from: http://download.microsoft.com/download/3/9/C/39C7DB36-2F55-4FD7-BD4C-EBBB58A2A21D/WindowsServer2003-KB893066-v2-x86-enu.exe

•Microsoft Windows Server 2003 < SP1 (x86), Microsoft Windows Server 2003, Standard Edition < SP1 (x86), Microsoft Windows Server 2003, Enterprise Edition < SP1 (x86), Microsoft Windows Server 2003, Datacenter Edition < SP1 (x86), Microsoft Windows Server 2003, Web Edition < SP1 (x86), Microsoft Windows Small Business Server 2003 < SP1 (x86)

Download and install Microsoft patch WindowsServer2003-KB893066-v2-x86-enu.exe (697584 bytes)

Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsserver2003-kb893066-v2-x86-enu_ed6adba942906756fec6fea17347ba1a526c594b.exe

•Microsoft Windows 2000 SP4 OR SP3 (x86), Microsoft Windows 2000 Professional SP4 OR SP3 (x86), Microsoft Windows 2000 Server SP4 OR SP3 (x86), Microsoft Windows 2000 Advanced Server SP4 OR SP3 (x86), Microsoft Windows 2000 Datacenter Server SP4 OR SP3 (x86)

Download and install Microsoft patch Windows2000-KB893066-v2-x86-ENU.EXE (756728 bytes)

Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windows2000-kb893066-v2-x86-enu_a5b95ec14e70e531e784ea83e633d24a0ea83795.exe

•Microsoft Windows XP Professional SP2 OR SP1 (x86), Microsoft Windows XP Home SP2 OR SP1 (x86)

Download and install Microsoft patch WindowsXP-KB893066-v2-x86-ENU.exe (791280 bytes)

Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb893066-v2-x86-enu_3d2029a4300c0b7943b20c1287c8143087045d52.exe

•Microsoft Windows Server 2003 SP1 OR < SP1 (x86), Microsoft Windows Server 2003, Standard Edition SP1 OR < SP1 (x86), Microsoft Windows Server 2003, Enterprise Edition SP1 OR < SP1 (x86), Microsoft Windows Server 2003, Datacenter Edition SP1 OR < SP1 (x86), Microsoft Windows Server 2003, Web Edition SP1 OR < SP1 (x86), Microsoft Windows Small Business Server 2003 SP1 OR < SP1 (x86)

Download and install Microsoft patch WindowsServer2003-KB922819-x86-ENU.exe (676664 bytes)

Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsserver2003-kb922819-x86-enu_22c5d80f99afb4a79b6245a4b5db1e8c95cb03fa.exe

- Microsoft Windows Server 2003 SP1 (x86_64), Microsoft Windows Server 2003, Standard Edition SP1 (x86_64), Microsoft Windows Server 2003, Enterprise Edition SP1 (x86_64), Microsoft Windows Server 2003, Datacenter Edition SP1 (x86_64), Microsoft Windows Server 2003, Web Edition SP1 (x86_64), Microsoft Windows Small Business Server 2003 SP1 (x86_64)
  Download and install Microsoft patch WindowsServer2003.WindowsXP-KB922819-x64-ENU.exe (898360 bytes)
  Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsserver2003.windowsxp-kb922819-x64-enu_4c34629b0664f2d2cd78c0276e4bd6b5e72ede61.exe
- Microsoft Windows XP Professional SP1 OR SP2 (x86), Microsoft Windows XP Home SP1 OR SP2 (x86)
  Download and install Microsoft patch WindowsXP-KB922819-x86-ENU.exe (856376 bytes)
  Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb922819-x86-enu_e4dceecdd4a72e5ad91cc78fe5f4572f91ee5db0.exe
- Microsoft Windows Server 2003 SP1 OR < SP1 (ia64), Microsoft Windows Server 2003, Standard Edition SP1 OR < SP1 (ia64), Microsoft Windows Server 2003, Enterprise Edition SP1 OR < SP1 (ia64), Microsoft Windows Server 2003, Datacenter Edition SP1 OR < SP1 (ia64), Microsoft Windows Server 2003, Web Edition SP1 OR < SP1 (ia64), Microsoft Windows Small Business Server 2003 SP1 OR < SP1 (ia64)
  Download and install Microsoft patch WindowsServer2003-KB922819-ia64-ENU.exe (1622328 bytes)
  Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsserver2003-kb922819-ia64-enu_34ecda284c6fc7b6fbbbfd6e2c823525ab9c838a.exe
- Microsoft Windows XP Professional SP1 (x86_64)
  Download and install Microsoft patch WindowsServer2003.WindowsXP-KB922819-x64-ENU.exe (898360 bytes)
  Download and apply the patch from: http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsserver2003.windowsxp-kb922819-x64-enu_4c34629b0664f2d2cd78c0276e4bd6b5e72ede61.exe
- Enable TCP MD5 Signatures
  Enable the TCP MD5 signature option as documented in RFC 2385. It was designed to reduce the danger from certain security attacks on BGP, such as TCP resets.

- Locate and fix vulnerable traffic inspection devices along the route to the target
  In many situations, target systems are, by themselves, patched or otherwise unaffected by this vulnerability. In certain configurations, however, unaffected systems can be made vulnerable if the path between an attacker and the target system contains an affected and unpatched network device such as a firewall or router and that device is responsible for handling TCP connections for the target. In this case, locate and apply remediation steps for network devices along the route that are affected.

3.2.63. Apache HTTPD: mod_proxy_balancer CSRF (CVE-2007-6420) (apache-httpd-cve-2007-6420)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running module mod_proxy_balancer. Review your Web server configuration for validation.The mod_proxy_balancer provided an administrative interface that could be vulnerable to cross-site request forgery (CSRF) attacks.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2008-10-09
BID	27236
BID	31681
CVE	CVE-2007-6420
OVAL	OVAL8371
REDHAT	RHSA-2008:0966
SECUNIA	31026
SECUNIA	32222
SECUNIA	33797
SECUNIA	34219
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.2 and < 2.2.9

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.9.tar.gz

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.64. Apache HTTPD: mod_proxy_ftp globbing XSS (CVE-2008-2939) (apache-httpd-cve-2008-2939)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running module mod_proxy_ftp. Review your Web server configuration for validation.A flaw was found in the handling of wildcards in the path of a FTP URL with mod_proxy_ftp. If mod_proxy_ftp is enabled to support FTP-over-HTTP, requests containing globbing characters could lead to cross-site scripting (XSS) attacks.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2009-05-12
BID	30560
CERT	TA09-133A
CERT-VN	663763
CVE	CVE-2008-2939

Source	Reference
OVAL	OVAL11316
OVAL	OVAL7716
REDHAT	RHSA-2008:0966
REDHAT	RHSA-2008:0967
SECUNIA	31384
SECUNIA	31673
SECUNIA	32685
SECUNIA	32838
SECUNIA	33156
SECUNIA	33797
SECUNIA	34219
SECUNIA	35074
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html
XF	apache-modproxyftp-xss(44223)

Vulnerability Solution:

•Apache >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache >= 2.2 and < 2.2.10

Upgrade to Apache HTTPD version 2.2.10

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.10.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.65. Apache HTTPD: APR-util heap underwrite (CVE-2009-0023) (apache-httpd-cve-2009-0023)

Description:

The affected asset is vulnerable to this vulnerability ONLY if an attacker can provide a specially crafted search keyword to a function that handles compiled forms of search patterns. Review your Web server configuration for validation.The affected asset is vulnerable to this vulnerability ONLY if an attacker can provide a specially crafted search keyword to a function that handles compiled forms of search patterns. Review your Web server configuration for validation.A heap-based underwrite flaw was found in the way the bundled copy of the APR-util library created compiled forms of particular search patterns. An attacker could formulate a specially-crafted search keyword, that would overwrite arbitrary heap memory locations when processed by the pattern preparation engine.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2009-11-09-1
BID	35221
CVE	CVE-2009-0023
DEBIAN	DSA-1812
OVAL	OVAL10968
OVAL	OVAL12321
REDHAT	RHSA-2009:1107
REDHAT	RHSA-2009:1108
SECUNIA	34724
SECUNIA	35284
SECUNIA	35360
SECUNIA	35395
SECUNIA	35444
SECUNIA	35487
SECUNIA	35565
SECUNIA	35710
SECUNIA	35797
SECUNIA	35843
SECUNIA	37221
URL	http://httpd.apache.org/security/vulnerabilities_22.html
XF	apache-aprstrmatchprecompile-dos(50964)

Vulnerability Solution:

Apache >= 2.2 and < 2.2.12

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.66. Apache HTTPD: Subrequest handling of request headers (mod_headers) (CVE-2010-0434) (apache-httpd-cve-2010-0434)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running module mod_headers. Review your Web server configuration for validation.A flaw in the core subrequest process code was fixed, to always provide a shallow copy of the headers_in array to the subrequest, instead of a pointer to the parent request's array as it had for requests without request bodies. This meant all modules such as mod_headers which may manipulate the input headers for a subrequest would poison the parent request in two ways, one by modifying the parent request, which might not be intended, and second by leaving pointers to modified header fields in memory allocated to the subrequest scope, which could be freed before the main request processing was finished, resulting in a segfault or in revealing data from another request on threaded servers, such as the worker or winnt MPMs.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2010-11-10-1
BID	38494
CVE	CVE-2010-0434
DEBIAN	DSA-2035
OVAL	OVAL10358
OVAL	OVAL8695
REDHAT	RHSA-2010:0168
REDHAT	RHSA-2010:0175
SECUNIA	39100
SECUNIA	39115
SECUNIA	39501
SECUNIA	39628
SECUNIA	39632
SECUNIA	39656
SECUNIA	40096
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html
XF	apache-http-rh-info-disclosure(56625)

Vulnerability Solution:

•Apache >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache >= 2.2 and < 2.2.15

Upgrade to Apache HTTPD version 2.2.15

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.67. Apache HTTPD: apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpd-cve-2011-0419)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running module mod_autoindex. Review your Web server configuration for validation.A flaw was found in the apr_fnmatch() function of the bundled APR library. Where mod_autoindex is enabled, and a directory indexed by mod_autoindex contained files with sufficiently long names, a remote attacker could send a carefully crafted request which would cause excessive CPU usage. This could be used in a denial of service attack. Workaround: Setting the 'IgnoreClient' option to the 'IndexOptions' directive disables processing of the client-supplied request query arguments, preventing this attack. Resolution: Update APR to release 0.9.20 (to be bundled with httpd 2.0.65)

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
CVE	CVE-2011-0419
DEBIAN	DSA-2237
IAVM	2012-B-0056
REDHAT	RHSA-2011:0507
REDHAT	RHSA-2011:0896
REDHAT	RHSA-2011:0897
SECUNIA	44490
SECUNIA	44564
SECUNIA	44574
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache >= 2.0 and < 2.0.65

Upgrade to Apache HTTPD version 2.0.65

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache >= 2.2 and < 2.2.19

Upgrade to Apache HTTPD version 2.2.19

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.19.tar.gz

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.68. Apache HTTPD: mod_setenvif .htaccess privilege escalation (CVE-2011-3607) (apache-httpd-cve-2011-3607)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running module mod_setenvif. Review your Web server configuration for validation.An integer overflow flaw was found which, when the mod_setenvif module is enabled, could allow local users to gain privileges via a .htaccess file.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	50494
CVE	CVE-2011-3607
IAVM	2012-A-0017
OSVDB	76744
REDHAT	RHSA-2012:0128
SECUNIA	45793
URL	http://httpd.apache.org/security/vulnerabilities_22.html
XF	apache-http-appregsub-bo(71093)

Vulnerability Solution:

Apache >= 2.2 and < 2.2.22

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.69. Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-4317) (apache-httpd-cve-2011-4317)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running module mod_proxy. Review your Web server configuration for validation.An additional exposure was found when using mod_proxy in reverse proxy mode. In certain configurations using RewriteRule with proxy flag or ProxyPassMatch, a remote attacker could cause the reverse proxy to connect to an arbitrary server, possibly disclosing sensitive information from internal web servers not directly accessible to attacker.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
CVE	CVE-2011-4317
IAVM	2012-A-0017
REDHAT	RHSA-2012:0128
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.2 and < 2.2.22

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.70. Apache HTTPD: error responses can expose cookies (CVE-2012-0053) (apache-httpd-cve-2012-0053)

Description:

A flaw was found in the default error response for status code 400. This flaw could be used by an attacker to expose "httpOnly" cookies when no custom ErrorDocument is specified.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	51706
CVE	CVE-2012-0053

Source	Reference
IAVM	2012-A-0017
REDHAT	RHSA-2012:0128
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

Apache >= 2.2 and < 2.2.22

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.2.71. Apache Tomcat v4.x Example Scripts Information Leakage (apache-tomcat-example-leaks)

Description:

The following example scripts that come with Apache Tomcat v4.x and can be used by attackers to gain information about the system. These scripts are also known to be vulnerable to cross site scripting (XSS) injection.

•/examples/jsp/num/numguess.jsp

•/examples/jsp/dates/date.jsp

•/examples/jsp/snp/snoop.jsp

•/examples/jsp/error/error.html

•/examples/jsp/sessions/carts.html

•/examples/jsp/checkbox/check.html

•/examples/jsp/colors/colors.html

•/examples/jsp/cal/login.html

•/examples/jsp/include/include.jsp

•/examples/jsp/forward/forward.jsp

•/examples/jsp/plugin/plugin.jsp

•/examples/jsp/jsptoserv/jsptoservlet.jsp

•/examples/jsp/simpletag/foo.jsp

•/examples/jsp/mail/sendmail.jsp

•/examples/servlet/HelloWorldExample

•/examples/servlet/RequestInfoExample

•/examples/servlet/RequestHeaderExample

•/examples/servlet/RequestParamExample

•/examples/servlet/CookieExample

•/examples/servlet/JndiServlet

•/examples/servlet/SessionExample

•/tomcat-docs/appdev/sample/web/hello.jsp

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.56.3:8180	Running vulnerable HTTP service: Apache Tomcat. http://192.168.56.3:8180/tomcat-docs/appdev/sample/web/hello.jsp 19: limitations under the License. 20: --> 21: <html> 22: <head> 19: <title>Sample Application JSP Page</title>

References:

None

Vulnerability Solution:

Delete these scripts entirely. Example scripts should never be installed on production servers.

3.2.72. BIND 9 DNSSEC validation code could cause bogus NXDOMAIN responses (dns-bind-cve-2010-0097)

Description:

There was an error in the DNSSEC NSEC/NSEC3 validation code that could cause bogus NXDOMAIN responses (that is, NXDOMAIN responses for records proven by NSEC or NSEC3 to exist) to be cached as if they had validated correctly, so that future queries to the resolver would return the bogus NXDOMAIN with the AD flag set. This problem affects all DNSSEC-validating resolvers. It would be difficult to exploit due to other existing protections against cache poisoning (including transaction ID and source port randomization), but it could impair the ability of DNSSEC to protect against a denial-of-service attack on a secure zone.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:53	Running vulnerable DNS service: BIND 9.4.2.

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
BID	37865
CERT-VN	360341
CVE	CVE-2010-0097
DEBIAN	DSA-2054
OSVDB	61853
OVAL	OVAL12205
OVAL	OVAL7212
OVAL	OVAL7430
OVAL	OVAL9357
REDHAT	RHSA-2010:0062
REDHAT	RHSA-2010:0095
SECUNIA	38169

Source	Reference
SECUNIA	38219
SECUNIA	38240
SECUNIA	39334
SECUNIA	39582
SECUNIA	40086
SUSE	SUSE-SA:2010:008
XF	bind-dnssecnsec-cache-poisoning(55753)

Vulnerability Solution:

•Upgrade to BIND version 9.4.3-P5

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.4.3-P5/bind-9.4.3-P5.tar.gz
Upgrade to 9.4.3-P5 version of ISC BIND Which was released on January 19, 2010. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.5.2-P2

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.5.2-P2/bind-9.5.2-P2.tar.gz
Upgrade to 9.5.2-P2 version of ISC BIND Which was released on January 19, 2010. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.6.1-P3

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.6.1-P3/bind-9.6.1-P3.tar.gz
Upgrade to 9.6.1-P3 version of ISC BIND Which was released on January 19, 2010. The source code and binaries for this release can be downloaded from bind's website.

3.2.73. BIND: cache incorrectly allows a ncache entry and a rrsig for the same type (dns-bind-cve-2010-3613)

Description:

Adding certain types of signed negative responses to cache doesn't clear any matching RRSIG records already in cache. A subsequent lookup of the cached data can cause named to crash (INSIST).

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:53	Running vulnerable DNS service: BIND 9.4.2.

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
BID	45133
CERT-VN	706148
CVE	CVE-2010-3613
DEBIAN	DSA-2130

Source	Reference
IAVM	2011-A-0066
NETBSD	NetBSD-SA2011-001
OSVDB	69558
OVAL	OVAL12601
REDHAT	RHSA-2010:0975
REDHAT	RHSA-2010:0976
REDHAT	RHSA-2010:1000
SECUNIA	42374
SECUNIA	42459
SECUNIA	42522
SECUNIA	42671
SECUNIA	42707
SECUNIA	43141

Vulnerability Solution:

•Upgrade to BIND version 9.4-ESV-R4

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.4-ESV-R4/bind-9.4-ESV-R4.tar.gz
Upgrade to 9.4-ESV-R4 version of ISC BIND Which was released on December 01, 2010. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.6-ESV-R3

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.6-ESV-R3/bind-9.6-ESV-R3.tar.gz
Upgrade to 9.6-ESV-R3 version of ISC BIND Which was released on December 01, 2010. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.6.2-P3

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.6.2-P3/bind-9.6.2-P3.tar.gz
Upgrade to 9.6.2-P3 version of ISC BIND Which was released on December 01, 2010. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.7.2-P3

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.7.2-P3/bind-9.7.2-P3.tar.gz
Upgrade to 9.7.2-P3 version of ISC BIND Which was released on December 01, 2010. The source code and binaries for this release can be downloaded from bind's website.

3.2.74. ISC BIND 9 Remote Dynamic Update Message Denial of Service Vulnerability (dns-bind-remote-dynamic-update-message-dos)

Description:

ISC BIND 9.4 before 9.4.3-P2, 9.5 before 9.5.1-P3, and 9.6 before 9.6.1-P1 ship with a flawed implementation of the dns_db_findrdataset function in db.c, when configured as a master server. This could allow remote attackers to cause a denial of service (assertion failure and daemon exit) via an ANY record in the prerequisite section of a crafted dynamic update message, as exploited in the wild in July 2009.

Affected Nodes:

Affected Nodes:	**Additional Information:**
192.168.56.3:53	Running vulnerable DNS service: BIND 9.4.2.

References:

Source	**Reference**
CERT-VN	725188
CVE	CVE-2009-0696
NETBSD	NetBSD-SA2009-013
OVAL	OVAL10414
OVAL	OVAL12245
OVAL	OVAL7806
SECUNIA	36035
SECUNIA	36038
SECUNIA	36050
SECUNIA	36053
SECUNIA	36056
SECUNIA	36063
SECUNIA	36086
SECUNIA	36098
SECUNIA	36192
SECUNIA	37471
SECUNIA	39334

Vulnerability Solution:

•Upgrade to BIND version 9.4.3-P3

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.4.3-P3/bind-9.4.3-P3.tar.gz
Upgrade to 9.4.3-P3 version of ISC BIND Which was released on July 29, 2009. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.5.1-P3

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.5.1-P3/bind-9.5.1-P3.tar.gz
Upgrade to 9.5.1-P3 version of ISC BIND Which was released on July 29, 2009. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.6.1-P1

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.6.1-P1/bind-9.6.1-P1.tar.gz
Upgrade to 9.6.1-P1 version of ISC BIND Which was released on July 29, 2009. The source code and binaries for this release can be downloaded from bind's website.

3.2.75. PHP Multiple Vulnerabilities Fixed in version 5.2.10 (http-php-multiple-vulns-5-2-10)

Description:

PHP versions before 5.2.10 can segfault on certain corrupted jpeg files in exit_read_data().

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
BID	35440
CVE	CVE-2009-2687
DEBIAN	DSA-1940
OSVDB	55222
OVAL	OVAL10695
OVAL	OVAL6655
SECUNIA	35441
SECUNIA	36462
SECUNIA	37482
SECUNIA	40262
URL	http://www.php.net/ChangeLog-5.php#5.2.10
URL	http://www.php.net/releases/5_2_10.php
XF	php-exifreaddata-dos(51253)

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.10.tar.gz
Upgrade to PHP v5.2.10 (released on June 18th, 2009).

3.2.76. MySQL Bug #29908: ALTER VIEW Privilege Escalation Vulnerability (mysql-bug-29908-alter-view-priv-esc)

Description:

A flaw in the ALTER VIEW routine of MySQL allows for the opportunity of an authenticated user to elevate their privileges in certain contexts.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:3306	Running vulnerable MySQL service: MySQL 5.0.51a.

References:

Source	Reference
URL	http://bugs.mysql.com/bug.php?id=29908

Vulnerability Solution:

•MySQL >= 5.0.0 and < 5.0.52

Upgrade to MySQL v5.0.52

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.0.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•MySQL (?:^5.1.)

Upgrade to MySQL v5.1.23

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.1.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.77. MySQL Bug #44798: Stored Procedures Server Crash (mysql-bug-44798-stored-procedures-server-crash)

Description:

Versions of MySQL server 5.0 before 5.0.84 and 5.1 before 5.1.36 suffer from a privilege interpretation flaw that causes a server crash. A user created with the privileges to create stored procedures but not execute them will trigger this issue.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:3306	Running vulnerable MySQL service: MySQL 5.0.51a.

References:

Source	Reference
URL	http://bugs.mysql.com/bug.php?id=44798

Vulnerability Solution:

•MySQL >= 5.0.0 and < 5.0.84

Upgrade to MySQL v5.0.84

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.0.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•MySQL (?:^5.1.)

Upgrade to MySQL v5.1.36

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.1.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.78. MySQL Empty Bit-String Literal Denial of Service (mysql-empty-bit-string-dos)

Description:

Certain versions of MySQL do not correctly handle SQL requests containing empty literal bit-string, such as:

```
    select b'';
```

This could allow a remote authenticated user to crash the service.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:3306	Running vulnerable MySQL service: MySQL 5.0.51a.

References:

Source	Reference
CVE	CVE-2008-3963
DEBIAN	DSA-1783
OVAL	OVAL10521
REDHAT	RHSA-2009:1067
SECUNIA	31769
SECUNIA	32759
SECUNIA	34907
URL	http://bugs.mysql.com/bug.php?id=35658
XF	mysql-bitstring-dos(45042)

Vulnerability Solution:

•MySQL (?:^5.0.)

Upgrade to MySQL v5.0.66

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.0.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•MySQL (?:^5.1.)

Upgrade to MySQL v5.1.26

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.1.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•MySQL (?:^6.0.)

Upgrade to MySQL v6.0.6

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/6.0.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.79. MySQL InnoDB Denial of Service (mysql-innodb-dos)

Description:

Certain versions of MySQL contain an assertion error within the InnoDB engine. The convert_search_mode_to_innobase function in ha_innodb.cc allows remote authenticated users to cause a denial of service (database crash) with a query using CONTAINS on a column that does not support SPATIAL indexes.

Affected Nodes:

Affected Nodes:	**Additional Information:**
192.168.56.3:3306	Running vulnerable MySQL service: MySQL 5.0.51a.

References:

Source	**Reference**
BID	26353
CVE	CVE-2007-5925
DEBIAN	DSA-1413
OVAL	OVAL11390
REDHAT	RHSA-2007:1155
REDHAT	RHSA-2007:1157
SECUNIA	27568
SECUNIA	27649
SECUNIA	27823
SECUNIA	28025
SECUNIA	28040
SECUNIA	28099
SECUNIA	28108
SECUNIA	28128
SECUNIA	28838
URL	http://bugs.mysql.com/bug.php?id=32125

Source	Reference
XF	mysql-hainnodb-dos(38284)

Vulnerability Solution:

•MySQL (?:^5.0.)

Upgrade to MySQL v5.0.24

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.0.html

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•MySQL (?:^5.1.)

Upgrade to MySQL v5.1.23

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.1.html

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

•MySQL (?:^6.0.)

Upgrade to MySQL v6.0.4

Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/6.0.html

Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.2.80. PHP Fixed possible attack in SSL sockets with SSL 3.0 / TLS 1.0 (php-cve-2011-3389)

Description:

The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-1
APPLE	APPLE-SA-2011-10-12-2
APPLE	APPLE-SA-2012-02-01-1
APPLE	APPLE-SA-2012-05-09-1
APPLE	APPLE-SA-2012-07-25-2

Source	Reference
BID	49388
BID	49778
CERT-VN	864643
CVE	CVE-2011-3389
IAVM	2012-A-0048
IAVM	2012-A-0085
IAVM	2012-B-0006
MS	MS12-006
OSVDB	74829
OVAL	OVAL14752
REDHAT	RHSA-2011:1384
REDHAT	RHSA-2012:0006
SECUNIA	45791

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.4.0.tar.gz
Upgrade to PHP v5.4.0.

3.2.81. PHP Fixed CVE-2012-2143 (php-cve-2012-2143)

Description:

The crypt_des (aka DES-based crypt) function in FreeBSD before 9.0-RELEASE-p2, as used in PHP, PostgreSQL, and other products, does not process the complete cleartext password if this password contains a 0x80 character, which makes it easier for context-dependent attackers to obtain access via an authentication attempt with an initial substring of the intended password, as demonstrated by a Unicode password.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
CVE	CVE-2012-2143
DEBIAN	DSA-2491
IAVM	2012-B-0061
REDHAT	RHSA-2012:1037

Vulnerability Solution:

•Upgrade to PHP v5.3.14

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.14.tar.gz

Upgrade to PHP v5.3.14.

•Upgrade to PHP v5.4.4

Download and apply the upgrade from: http://museum.php.net/php5/php-5.4.4.tar.gz
Upgrade to PHP v5.4.4.

3.2.82. PHP Fixed dl() to limit argument size to MAXPATHLEN (php-fixed-dl-to-limit-argument-size-to-maxpathlen)

Description:

The dl function in PHP 5.2.4 and earlier allows context-dependent attackers to cause a denial of service (application crash) via a long string in the library parameter. NOTE: there are limited usage scenarios under which this would be a vulnerability.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2008-03-18
BID	26403
CVE	CVE-2007-4887
OVAL	OVAL5767
SECUNIA	27102
SECUNIA	27659
SECUNIA	28750
SECUNIA	29420
SECUNIA	30040

Vulnerability Solution:

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.5.tar.gz
Upgrade to PHP v5.2.5.

3.2.83. PHP Fixed NULL pointer dereference in ZipArchive::getArchiveComment (php-fixed-null-pointer-dereference-in-ziparchivegetarchivecomment)

Description:

The ZipArchive::getArchiveComment function in PHP 5.2.x through 5.2.14 and 5.3.x through 5.3.3 allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ZIP archive.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2011-03-21-1
BID	44718
CVE	CVE-2010-3709
REDHAT	RHSA-2011:0195
SECUNIA	42729
SECUNIA	42812

Vulnerability Solution:

•Upgrade to PHP v5.3.4

Download and apply the upgrade from: http://museum.php.net/php5/php-5.3.4.tar.gz
Upgrade to PHP v5.3.4.

•Upgrade to PHP v5.2.15

Download and apply the upgrade from: http://museum.php.net/php5/php-5.2.15.tar.gz
Upgrade to PHP v5.2.15.

3.2.84. PHP Rewrote var_export() to use smart_str (php-rewrote-var-export-to-use-smart-str)

Description:

The var_export function in PHP 5.2 before 5.2.14 and 5.3 before 5.3.3 flushes the output buffer to the user when certain fatal errors occur, even if display_errors is off, which allows remote attackers to obtain sensitive information by causing the application to exceed limits for memory, execution time, or recursion.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
APPLE	APPLE-SA-2010-08-24-1
APPLE	APPLE-SA-2010-11-10-1
CVE	CVE-2010-2531
DEBIAN	DSA-2266

Source	Reference
REDHAT	RHSA-2010:0919
SECUNIA	42410

Vulnerability Solution:

•Upgrade to PHP v5.2.14

Download and apply the upgrade from: http://www.php.net/get/php-5.2.14.tar.gz/from/a/mirror
Upgrade to PHP v5.2.14.

•Upgrade to PHP v5.3.3

Download and apply the upgrade from: http://www.php.net/get/php-5.3.3.tar.gz/from/a/mirror
Upgrade to PHP v5.3.3.

3.2.85. Self-signed TLS/SSL certificate (ssl-self-signed-certificate)

Description:

The server's TLS/SSL certificate is self-signed. Self-signed certificates cannot be trusted by default, especially because TLS/SSL man-in-the-middle attacks typically use self-signed certificates to eavesdrop on TLS/SSL connections.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:25	TLS/SSL certificate is self-signed.

References:

None

Vulnerability Solution:

Obtain a new TLS/SSL server certificate that is NOT self-signed and install it on the server. The exact instructions for obtaining a new certificate depend on your organization's requirements. Generally, you will need to generate a certificate request and save the request as a file. This file is then sent to a Certificate Authority (CA) for processing. Your organization may have its own internal Certificate Authority. If not, you may have to pay for a certificate from a trusted external Certificate Authority, such as Thawte or Verisign.

3.3. Moderate Vulnerabilities

3.3.1. Apache HTTPD: mod_proxy_ftp DoS (CVE-2009-3094) (apache-httpd-cve-2009-3094)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running module mod_proxy_ftp. Review your Web server configuration for validation.A NULL pointer dereference flaw was found in the mod_proxy_ftp module. A malicious FTP server to which requests are being proxied could use this flaw to crash an httpd child process via a malformed reply to the EPSV or PASV commands, resulting in a limited denial of service.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:80	Running vulnerable HTTP service: Apache 2.2.8.

References:

Source	Reference
CVE	CVE-2009-3094
DEBIAN	DSA-1934
OVAL	OVAL10981
OVAL	OVAL8087
SECUNIA	36549
SECUNIA	37152
SUSE	SUSE-SA:2009:050
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Vulnerability Solution:

•Apache >= 2.0 and < 2.0.64

Upgrade to Apache HTTPD version 2.0.64

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache >= 2.2 and < 2.2.14

Upgrade to Apache HTTPD version 2.2.14

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.3.2. ISC BIND DNSSEC Cache Poisoning Vulnerability (dns-bind9-dnssec-cache-poisoning)

Description:

ISC BIND 9.4 before 9.4.3-P4, 9.5 before 9.5.2-P1, 9.6 before 9.6.1-P2, 9.7 beta before 9.7.0b3, and 9.0.x through 9.3.x with DNSSEC validation enabled and checking disabled (CD), allows remote attackers to conduct DNS cache poisoning attacks via additional sections in a response sent for resolution of a recursive client query, which is not properly handled when the response is processed at the same time as requesting DNSSEC records (DO).

Affected Nodes:

Affected Nodes:	Additional Information:

Affected Nodes:	Additional Information:
192.168.56.3:53	Running vulnerable DNS service: BIND 9.4.2.

References:

Source	Reference
APPLE	APPLE-SA-2011-10-12-3
BID	37118
CERT-VN	418861
CVE	CVE-2009-4022
OSVDB	60493
OVAL	OVAL10821
OVAL	OVAL11745
OVAL	OVAL7261
OVAL	OVAL7459
REDHAT	RHSA-2009:1620
SECUNIA	37426
SECUNIA	37491
SECUNIA	38219
SECUNIA	38240
SECUNIA	38794
SECUNIA	38834
SECUNIA	39334
SECUNIA	40730
URL	https://www.isc.org/advisories/CVE2009-4022
XF	bind-dnssec-cache-poisoning(54416)

Vulnerability Solution:

•Upgrade to BIND version 9.4.3-P5

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.4.3-P5/bind-9.4.3-P5.tar.gz
Upgrade to 9.4.3-P5 version of ISC BIND Which was released on January 19, 2010. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.5.2-P2

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.5.2-P2/bind-9.5.2-P2.tar.gz
Upgrade to 9.5.2-P2 version of ISC BIND Which was released on January 19, 2010. The source code and binaries for this release can be downloaded from bind's website.

•Upgrade to BIND version 9.6.1-P3

Download and apply the upgrade from: http://ftp.isc.org/isc/bind9/9.6.1-P3/bind-9.6.1-P3.tar.gz
Upgrade to 9.6.1-P3 version of ISC BIND Which was released on January 19, 2010. The source code and binaries for this release can be downloaded from bind's website.

3.3.3. MySQL HTML Output Script Insertion Vulnerability (mysql-html-output-script-insertion)

Description:

A cross-site scripting (XSS) vulnerability exists in the command-line client when the "--html" option is enabled. This could allow attackers to inject arbitrary web script or HTML by placing it in a database cell, which might be accessed by the client when composing an HTML document.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:3306	Running vulnerable MySQL service: MySQL 5.0.51a.

References:

Source	Reference
APPLE	APPLE-SA-2010-03-29-1
BID	31486
CVE	CVE-2008-4456
DEBIAN	DSA-1783
OVAL	OVAL11456
REDHAT	RHSA-2010:0110
SECUNIA	32072
SECUNIA	34907
SECUNIA	38517
URL	http://bugs.mysql.com/bug.php?id=27884
URL	http://www.henlich.de/it-security/mysql-command-line-client-html-injection-vulnerability
XF	mysql-commandline-xss(45590)

Vulnerability Solution:

MySQL (?:^5.1.)
Download and apply the upgrade from: http://dev.mysql.com/downloads/mysql/5.1.html
Please note that individual platforms and OS distributions may provide their own means of upgrading MySQL (via an RPM, for example). These supported upgrade methods should be used if available, instead of building the distribution from scratch.

3.3.4. Unencrypted Telnet Service Available (telnet-open-port)

Description:

Telnet is an unencrypted protocol, as such it sends sensitive data (usernames and passwords) in clear text. For this reason, it is a violation of PCI DSS section 2.3 to have telnet enabled, unless a business case can be made for why it is required.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:23	Running vulnerable Telnet service.

References:

Source	Reference
URL	https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-2.pdf

Vulnerability Solution:

Disable the telnet service. Replace it with technologies such as SSH, VPN, or TLS.

3.3.5. Weak Cryptographic Key (weak-crypto-key)

Description:

The key length used by a cryptographic algorithm determines the highest security it can offer. Newly discovered theoretical attacks and hardware advances constantly erode this security level over time. Taking this into account, as of 2011, governmental, academic, and private organizations providing guidance on cryptographic security, such as the National Institute of Standards and Technology (NIST), the European Network of Excellence in Cryptology II (ECRYPT II), make the following general recommendations to provide short to medium term security against even the most well-funded attackers (eg. intelligence agencies):

- Symmetric key lengths of at least 80-112 bits.
- Elliptic curve key lengths of at least 160-224 bits.
- RSA key lengths of at least 1248-2048 bits. In particular, the CA/Browser Forum Extended Validation (EV) Guidelines require a minimum key length of 2048 bits. Also, current research shows that factoring a 1024-bit RSA modulus is within practical reach.
- DSA key lengths of at least 2048 bits.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:25	Length of RSA modulus in X.509 certificate: 1024 bits (less than 2047 bits)

References:

Source	Reference
URL	http://csrc.nist.gov/groups/ST/toolkit/key_management.html
URL	http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2011_2_AlgoKatpdf.pdf
URL	http://www.ecrypt.eu.org/documents/D.SPA.17.pdf
URL	http://www.keylength.com
URL	http://www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf

Vulnerability Solution:

If the weak key is used in an X.509 certificate (for example for an HTTPS server), generate a longer key and recreate the certificate.

3.3.6. Apache Tomcat default installation/welcome page installed (apache-tomcat-default-install-page)

Description:

The Tomcat default installation or "Welcome" page is installed on this server. This usually indicates a newly installed server which has not yet been configured properly and which may not be known about.

In many cases, Tomcat is installed along with other applications and the user may not be aware that the web server is running. These servers are rarely patched and rarely monitored, providing hackers with a convenient target that is not likely to trip any alarms.

Affected Nodes:

Affected Nodes:	Additional Information:

192.168.56.3:8180	Running vulnerable HTTP service: Apache Tomcat.
	http://192.168.56.3:8180/
	`194:         <td style="width:20px">&nbsp;</td>`
	`195:`
	`196:         <!-- Body -->`
	`197:         <td align="left" valign="top">`
	`194: ... means you've` setup Tomcat successfully. Congratulations
	`!</p>`

References:

Source	Reference
OSVDB	2117

Vulnerability Solution:

If this server is required to provide necessary functionality, then the default page should be replaced with relevant content. Otherwise, this server should be removed from the network, following the security principle of minimum complexity.

3.3.7. FTP access with ftp account (ftp-generic-0001)

Description:

Many FTP servers support a default account with the user ID "ftp" and password "ftp". It is best practice to remove default accounts, if possible. For accounts required by the system, the default password should be changed.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:21	Running vulnerable FTP service. Successfully authenticated to the FTP service with credentials: uid[ftp] pw[ftp] realm[null]

References:

Source	Reference

Source	Reference
CVE	CVE-1999-0497

Vulnerability Solution:

Remove or disable the account if it is not critical for the system to function. Otherwise, the password should be changed to a non-default value.

3.3.8. FTP access with anonymous account (ftp-generic-0002)

Description:

Many FTP servers support a default account with the user ID "anonymous" and password "ftp@". It is best practice to remove default accounts, if possible. For accounts required by the system, the default password should be changed.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:21	Running vulnerable FTP service. Successfully authenticated to the FTP service with credentials: uid[anonymous] pw[joe@] realm[null]

References:

Source	Reference
CVE	CVE-1999-0497

Vulnerability Solution:

Remove or disable the account if it is not critical for the system to function. Otherwise, the password should be changed to a non-default value.

3.3.9. ICMP timestamp response (generic-icmp-timestamp)

Description:

The remote host responded to an ICMP timestamp request. The ICMP timestamp response contains the remote host's date and time. This information could theoretically be used against some systems to exploit weak time-based random number generators in other services.

In addition, the versions of some operating systems can be accurately fingerprinted by analyzing their responses to invalid ICMP timestamp requests.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3	Remote system time: 01:06:41.040 EST

References:

Source	Reference
CVE	CVE-1999-0524

Source	Reference
OSVDB	95
XF	icmp-netmask(306)
XF	icmp-timestamp(322)

Vulnerability Solution:

•HP-UX

Disable ICMP timestamp responses on HP/UX

Execute the following command:

```
ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Cisco IOS

Disable ICMP timestamp responses on Cisco IOS

Use ACLs to block ICMP types 13 and 14. For example:

```
deny icmp any any 13
deny icmp any any 14
```

Note that it is generally preferable to use ACLs that block everything by default and then selectively allow certain types of traffic in. For example, block everything and then only allow ICMP unreachable, ICMP echo reply, ICMP time exceeded, and ICMP source quench:

```
permit icmp any any unreachable
permit icmp any any echo-reply
permit icmp any any time-exceeded
permit icmp any any source-quench
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•SGI Irix

Disable ICMP timestamp responses on SGI Irix

IRIX does not offer a way to disable ICMP timestamp responses. Therefore, you should block ICMP on the affected host using ipfilterd, and/or block it at any external firewalls.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Linux

Disable ICMP timestamp responses on Linux

Linux offers neither a sysctl nor a /proc/sys/net/ipv4 interface to disable ICMP timestamp responses. Therefore, you should block ICMP on the affected host using iptables, and/or block it at the firewall. For example:

```
ipchains -A input -p icmp --icmp-type timestamp-request -j DROP
ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Microsoft Windows NT, Microsoft Windows NT Workstation, Microsoft Windows NT Server, Microsoft Windows NT Advanced Server, Microsoft Windows NT Server, Enterprise Edition, Microsoft Windows NT Server, Terminal Server Edition

Disable ICMP timestamp responses on Windows NT 4

Windows NT 4 does not provide a way to block ICMP packets. Therefore, you should block them at the firewall.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•OpenBSD

Disable ICMP timestamp responses on OpenBSD

Set the "net.inet.icmp.tstamprepl" sysctl variable to 0.

```
sysctl -w net.inet.icmp.tstamprepl=0
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Cisco PIX

Disable ICMP timestamp responses on Cisco PIX

A properly configured PIX firewall should never respond to ICMP packets on its external interface. In PIX Software versions 4.1(6) until 5.2.1, ICMP traffic to the PIX's internal interface is permitted; the PIX cannot be configured to NOT respond. Beginning in PIX Software version 5.2.1, ICMP is still permitted on the internal interface by default, but ICMP responses from its internal interfaces can be disabled with the icmp command, as follows, where <inside> is the name of the internal interface:

```
icmp deny any 13 <inside>
icmp deny any 14 <inside>
```

Don't forget to save the configuration when you are finished.

See Cisco's support document Handling ICMP Pings with the PIX Firewall for more information.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Sun Solaris

Disable ICMP timestamp responses on Solaris

Execute the following commands:

```
/usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp 0
/usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
```

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

•Microsoft Windows 2000, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server

Disable ICMP timestamp responses on Windows 2000

Use the IPSec filter feature to define and apply an IP filter list that blocks ICMP types 13 and 14. Note that the standard TCP/IP blocking capability under the "Networking and Dialup Connections" control panel is NOT capable of blocking ICMP (only TCP and UDP). The IPSec filter features, while they may seem strictly related to the IPSec standards, will allow you to selectively block these ICMP packets. See http://support.microsoft.com/kb/313190 for more information.

The easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

- Microsoft Windows XP, Microsoft Windows XP Home, Microsoft Windows XP Professional, Microsoft Windows Server 2003, Microsoft Windows Server 2003, Standard Edition, Microsoft Windows Server 2003, Enterprise Edition, Microsoft Windows Server 2003, Datacenter Edition, Microsoft Windows Server 2003, Web Edition, Microsoft Windows Small Business Server 2003
Disable ICMP timestamp responses on Windows XP/2K3
ICMP timestamp responses can be disabled by deselecting the "allow incoming timestamp request" option in the ICMP configuration panel of Windows Firewall.
1. Go to the Network Connections control panel.
2. Right click on the network adapter and select "properties", or select the internet adapter and select File->Properties.
3. Select the "Advanced" tab.
4. In the Windows Firewall box, select "Settings".
5. Select the "General" tab.
6. Enable the firewall by selecting the "on (recommended)" option.
7. Select the "Advanced" tab.
8. In the ICMP box, select "Settings".
9. Deselect (uncheck) the "Allow incoming timestamp request" option.
10. Select "OK" to exit the ICMP Settings dialog and save the settings.
11. Select "OK" to exit the Windows Firewall dialog and save the settings.
12. Select "OK" to exit the internet adapter dialog.
For more information, see: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw_understanding_firewall.mspx?mfr=true

- Microsoft Windows Vista, Microsoft Windows Vista Home, Basic Edition, Microsoft Windows Vista Home, Basic N Edition, Microsoft Windows Vista Home, Premium Edition, Microsoft Windows Vista Ultimate Edition, Microsoft Windows Vista Enterprise Edition, Microsoft Windows Vista Business Edition, Microsoft Windows Vista Business N Edition, Microsoft Windows Vista Starter Edition, Microsoft Windows Server 2008, Microsoft Windows Server 2008 Standard Edition, Microsoft Windows Server 2008 Enterprise Edition, Microsoft Windows Server 2008 Datacenter Edition, Microsoft Windows Server 2008 HPC Edition, Microsoft Windows Server 2008 Web Edition, Microsoft Windows Server 2008 Storage Edition, Microsoft Windows Small Business Server 2008, Microsoft Windows Essential Business Server 2008
Disable ICMP timestamp responses on Windows Vista/2008
ICMP timestamp responses can be disabled via the netsh command line utility.
1. Go to the Windows Control Panel.
2. Select "Windows Firewall".
3. In the Windows Firewall box, select "Change Settings".
4. Enable the firewall by selecting the "on (recommended)" option.
5. Open a Command Prompt.
6. Enter "netsh firewall set icmpsetting 13 disable"
For more information, see: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw_understanding_firewall.mspx?mfr=true

- Disable ICMP timestamp responses
Disable ICMP timestamp replies for the device. If the device does not support this level of configuration, the easiest and most effective solution is to configure your firewall to block incoming and outgoing ICMP packets with ICMP types 13 (timestamp request) and 14 (timestamp response).

3.3.10. TCP timestamp response (generic-tcp-timestamp)

Description:

The remote host responded with a TCP timestamp. The TCP timestamp response can be used to approximate the remote host's uptime, potentially aiding in further attacks. Additionally, some operating systems can be fingerprinted based on the behavior of their TCP timestamps.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3	Apparent system boot time: Mon Aug 20 05:33:48 EST 2012

References:

Source	Reference
URL	http://uptime.netcraft.com
URL	http://www.forensicswiki.org/wiki/TCP_timestamps
URL	http://www.ietf.org/rfc/rfc1323.txt

Vulnerability Solution:

•Cisco

Disable TCP timestamp responses on Cisco

Run the following command to disable TCP timestamps:

```
no ip tcp timestamp
```

•FreeBSD

Disable TCP timestamp responses on FreeBSD

Set the value of net.inet.tcp.rfc1323 to 0 by running the following command:

```
sysctl -w net.inet.tcp.rfc1323=0
```

Additionally, put the following value in the default sysctl configuration file, generally sysctl.conf:

```
net.inet.tcp.rfc1323=0
```

•Linux

Disable TCP timestamp responses on Linux

Set the value of net.ipv4.tcp_timestamps to 0 by running the following command:

```
sysctl -w net.ipv4.tcp_timestamps=0
```

Additionally, put the following value in the default sysctl configuration file, generally sysctl.conf:

```
net.ipv4.tcp_timestamps=0
```

•OpenBSD

Disable TCP timestamp responses on OpenBSD

Set the value of net.inet.tcp.rfc1323 to 0 by running the following command:

```
sysctl -w net.inet.tcp.rfc1323=0
```

Additionally, put the following value in the default sysctl configuration file, generally sysctl.conf:

```
net.inet.tcp.rfc1323=0
```

•Microsoft Windows

Disable TCP timestamp responses on Windows

Set the Tcp1323Opts value in the following key to 1:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
```

3.3.11. OpenSSH "X11UseLocalhost" X11 Forwarding Session Hijacking Vulnerability (ssh-openssh-x11uselocalhost-x11-forwarding-session-hijack)

Description:

Certain versions of OpenSSH set the SO_REUSEADDR socket option when the X11UseLocalhost configuration setting is disabled. This could allow a local attacker to hijack the X11 forwarding port via a bind to a single IP address.

Affected Nodes:

Affected Nodes:	Additional Information:
192.168.56.3:22	OpenSSH 4.7p1 on Ubuntu Linux 8.04

References:

Source	Reference
BID	30339
CVE	CVE-2008-3259
SECUNIA	31179
XF	openssh-x11forwarding-info-disclosure(43940)

Vulnerability Solution:

Download and apply the upgrade from: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-5.1p1.tar.gz
Version 5.1 of OpenSSH was released on July 21st, 2008.
While you can always build OpenSSH from source, many platforms and distributions provide pre-built binary packages for OpenSSH. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

3.3.12. UDP IP ID Zero (udp-ipid-zero)

Description:

The remote host responded with a UDP packet whose IP ID was zero. Normally the IP ID should be set to a unique value and is used in the reconstruction of fragmented packets. Generally this behavior is only seen with systems derived from a Linux kernel, which may allow an attacker to fingerprint the target's operating system.

Affected Nodes:

Affected Nodes:	**Additional Information:**
192.168.56.3	Received UDP packet with IP ID of zero:IPv4 SRC[192.168.56.3] TGT[192.168.56.1] TOS[0] TTL[64] Flags[40] Proto[17] ID[0] FragOff[0] HDR-LENGTH[20] TOTAL-LENGTH[52] CKSUM[18788] UDP SRC-PORT[48701] TGT-PORT[47159] CKSUM[29994] RAW DATA [24]: 3EECE3CA000000010000000000000000 >............ 0000000000000001 ....

References:

None

Vulnerability Solution:

Many vendors do not consider this to be a vulnerability, or a vulnerability worth fixing, so there are no vendor-provided solutions aside from putting a firewall or other filtering device between the target and hostile attackers that is capable of randomizing IP IDs.

4. Discovered Services

4.1. CIFS

CIFS, the Common Internet File System, was defined by Microsoft to provide file sharing services over the Internet. CIFS extends the Server Message Block (SMB) protocol designed by IBM and enhanced by Intel and Microsoft. CIFS provides mechanisms for sharing resources (files, printers, etc.) and executing remote procedure calls over named pipes.

4.1.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	tcp	139	6	•Samba 3.0.20-Debian
192.168.56.3	tcp	445	6	•Samba 3.0.20-Debian

4.2. CIFS Name Service

CIFS, the Common Internet File System, was defined by Microsoft to provide file sharing services over the Internet. CIFS extends the Server Message Block (SMB) protocol designed by IBM and enhanced by Intel and Microsoft. CIFS provides mechanisms for sharing resources (files, printers, etc.) and executing remote procedure calls over named pipes. This service is used to handle CIFS browsing (name) requests. Responses contain the names and types of services that can be accessed via CIFS named pipes.

4.2.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	udp	137	0	•advertised-name-1: METASPLOITABLE (Computer Name) •advertised-name-2: METASPLOITABLE (Logged-on User) •advertised-name-3: METASPLOITABLE (File Server Service) •advertised-name-4: __MSBROWSE__ (Master Browser) •advertised-name-5: WORKGROUP (Domain Name) •advertised-name-6: WORKGROUP (Master Browser) •advertised-name-7: WORKGROUP (Browser Service Elections) •advertised-name-count: 7 •mac-address: 000000000000

4.3. DNS

DNS, the Domain Name System, provides naming services on the Internet. DNS is primarily used to convert names, such as www.rapid7.com to their corresponding IP address for use by network programs, such as a browser.

4.3.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	udp	53	6	•BIND 9.4.2

4.4. DNS-TCP

DNS, the Domain Name System, provides naming services on the Internet. DNS is primarily used to convert names, such as www.rapid7.com to their corresponding IP address for use by network programs, such as a browser. This service is used primarily for zone transfers between DNS servers. It can, however, be used for standard DNS queries as well.

4.4.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	tcp	53	0	•BIND 9.4.2

4.5. FTP

FTP, the File Transfer Protocol, is used to transfer files between systems. On the Internet, it is often used on web pages to download files from a web site using a browser. FTP uses two connections, one for control connections used to authenticate, navigate the FTP server and initiate file transfers. The other connection is used to transfer data, such as files or directory listings.

4.5.1. General Security Issues

Cleartext authentication

The original FTP specification only provided means for authentication with cleartext user ids and passwords. Though FTP has added support for more secure mechanisms such as Kerberos, cleartext authentication is still the primary mechanism. If a malicious user is in a position to monitor FTP traffic, user ids and passwords can be stolen.

4.5.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	tcp	21	2	•vsFTPd 2.3.4 •ftp.banner: 220 (vsFTPd 2.3.4)

4.6. HTTP

HTTP, the HyperText Transfer Protocol, is used to exchange multimedia content on the World Wide Web. The multimedia files commonly used with HTTP include text, sound, images and video.

4.6.1. General Security Issues

Simple authentication scheme

Many HTTP servers use BASIC as their primary mechanism for user authentication. This is a very simple scheme that uses base 64 to encode the cleartext user id and password. If a malicious user is in a position to monitor HTTP traffic, user ids and passwords can be stolen by decoding the base 64 authentication data. To secure the authentication process, use HTTPS (HTTP over TLS/SSL) connections to transmit the authentication data.

4.6.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	tcp	80	7	•Apache 2.2.8

Device	Protocol	Port	Vulnerabilities	Additional Information
				•DAV: 2 •PHP: 5.2.4-2ubuntu5.10 •WebDAV: •http.banner: Apache/2.2.8 (Ubuntu) DAV/2 •http.banner.server: Apache/2.2.8 (Ubuntu) DAV/2 •http.banner.x-powered-by: PHP/5.2.4-2ubuntu5.10
192.168.56.3	tcp	8180	3	•Apache Tomcat •Coyote: 1.1 •http.banner: Apache-Coyote/1.1 •http.banner.server: Apache-Coyote/1.1

4.7. MySQL

4.7.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	tcp	3306	7	•MySQL 5.0.51a •auto_increment_increment: 1 •auto_increment_offset: 1 •automatic_sp_privileges: ON •back_log: 50 •basedir: /usr/ •binlog_cache_size: 32768 •bulk_insert_buffer_size: 8388608 •character_set_client: latin1 •character_set_connection: latin1 •character_set_database: latin1 •character_set_filesystem: binary •character_set_results: •character_set_server: latin1 •character_set_system: utf8 •character_sets_dir: /usr/share/mysql/charsets/ •collation_connection: latin1_swedish_ci •collation_database: latin1_swedish_ci •collation_server: latin1_swedish_ci •completion_type: 0

Device	Protocol	Port	Vulnerabilities	Additional Information
				•concurrent_insert: 1 •connect_timeout: 5 •datadir: /var/lib/mysql/ •date_format: %Y-%m-%d •datetime_format: %Y-%m-%d %H:%i:%s •default_week_format: 0 •delay_key_write: ON •delayed_insert_limit: 100 •delayed_insert_timeout: 300 •delayed_queue_size: 1000 •div_precision_increment: 4 •engine_condition_pushdown: OFF •expire_logs_days: 10 •flush: OFF •flush_time: 0 •ft_boolean_syntax: + -><()~*:""&| •ft_max_word_len: 84 •ft_min_word_len: 4 •ft_query_expansion_limit: 20 •ft_stopword_file: (built-in) •group_concat_max_len: 1024 •have_archive: YES •have_bdb: NO •have_blackhole_engine: YES •have_compress: YES •have_crypt: YES •have_csv: YES •have_dynamic_loading: YES •have_example_engine: NO •have_federated_engine: YES •have_geometry: YES •have_innodb: YES •have_isam: NO •have_merge_engine: YES •have_ndbcluster: DISABLED •have_openssl: YES •have_query_cache: YES •have_raid: NO •have_rtree_keys: YES •have_ssl: YES •have_symlink: YES •hostname: metasploitable

Device	Protocol	Port	Vulnerabilities	Additional Information
				•init_connect: •init_file: •init_slave: •innodb_additional_mem_pool_size: 1048576 •innodb_autoextend_increment: 8 •innodb_buffer_pool_awe_mem_mb: 0 •innodb_buffer_pool_size: 8388608 •innodb_checksums: ON •innodb_commit_concurrency: 0 •innodb_concurrency_tickets: 500 •innodb_data_file_path: ibdata1:10M:autoextend •innodb_data_home_dir: •innodb_doublewrite: ON •innodb_fast_shutdown: 1 •innodb_file_io_threads: 4 •innodb_file_per_table: OFF •innodb_flush_log_at_trx_commit: 1 •innodb_flush_method: •innodb_force_recovery: 0 •innodb_lock_wait_timeout: 50 •innodb_locks_unsafe_for_binlog: OFF •innodb_log_arch_dir: •innodb_log_archive: OFF •innodb_log_buffer_size: 1048576 •innodb_log_file_size: 5242880 •innodb_log_files_in_group: 2 •innodb_log_group_home_dir: ./ •innodb_max_dirty_pages_pct: 90 •innodb_max_purge_lag: 0 •innodb_mirrored_log_groups: 1 •innodb_open_files: 300 •innodb_rollback_on_timeout: OFF •innodb_support_xa: ON •innodb_sync_spin_loops: 20 •innodb_table_locks: ON •innodb_thread_concurrency: 8 •innodb_thread_sleep_delay: 10000 •interactive_timeout: 28800 •join_buffer_size: 131072

Device	Protocol	Port	Vulnerabilities	Additional Information
				•keep_files_on_create: OFF •key_buffer_size: 16777216 •key_cache_age_threshold: 300 •key_cache_block_size: 1024 •key_cache_division_limit: 100 •language: /usr/share/mysql/english/ •large_files_support: ON •large_page_size: 0 •large_pages: OFF •lc_time_names: en_US •license: GPL •local_infile: ON •locked_in_memory: OFF •log: OFF •log_bin: OFF •log_bin_trust_function_creators: OFF •log_error: •log_queries_not_using_indexes: OFF •log_slave_updates: OFF •log_slow_queries: OFF •log_warnings: 1 •logging: disabled •long_query_time: 10 •low_priority_updates: OFF •lower_case_file_system: OFF •lower_case_table_names: 0 •max_allowed_packet: 16776192 •max_binlog_cache_size: 4294967295 •max_binlog_size: 104857600 •max_connect_errors: 10 •max_connections: 100 •max_delayed_threads: 20 •max_error_count: 64 •max_heap_table_size: 16777216 •max_insert_delayed_threads: 20 •max_join_size: 18446744073709551615 •max_length_for_sort_data: 1024 •max_prepared_stmt_count: 16382 •max_relay_log_size: 0 •max_seeks_for_key: 4294967295 •max_sort_length: 1024

Device	Protocol	Port	Vulnerabilities	Additional Information
				•max_sp_recursion_depth: 0 •max_tmp_tables: 32 •max_user_connections: 0 •max_write_lock_count: 4294967295 •multi_range_count: 256 •myisam_data_pointer_size: 6 •myisam_max_sort_file_size: 2147483647 •myisam_recover_options: OFF •myisam_repair_threads: 1 •myisam_sort_buffer_size: 8388608 •myisam_stats_method: nulls_unequal •ndb_autoincrement_prefetch_sz: 32 •ndb_cache_check_time: 0 •ndb_connectstring: •ndb_force_send: ON •ndb_use_exact_count: ON •ndb_use_transactions: ON •net_buffer_length: 16384 •net_read_timeout: 30 •net_retry_count: 10 •net_write_timeout: 60 •new: OFF •old_passwords: OFF •open_files_limit: 1024 •optimizer_prune_level: 1 •optimizer_search_depth: 62 •pid_file: /var/run/mysqld/mysqld.pid •port: 3306 •preload_buffer_size: 32768 •profiling: OFF •profiling_history_size: 15 •protocolVersion: 10 •protocol_version: 10 •query_alloc_block_size: 8192 •query_cache_limit: 1048576 •query_cache_min_res_unit: 4096 •query_cache_size: 16777216 •query_cache_type: ON •query_cache_wlock_invalidate: OFF •query_prealloc_size: 8192 •range_alloc_block_size: 2048

Device	Protocol	Port	Vulnerabilities	Additional Information
				•read_buffer_size: 131072 •read_only: OFF •read_rnd_buffer_size: 262144 •relay_log_purge: ON •relay_log_space_limit: 0 •rpl_recovery_rank: 0 •secure_auth: OFF •secure_file_priv: •server_id: 0 •skip_external_locking: ON •skip_networking: OFF •skip_show_database: OFF •slave_compressed_protocol: OFF •slave_load_tmpdir: /tmp/ •slave_net_timeout: 3600 •slave_skip_errors: OFF •slave_transaction_retries: 10 •slow_launch_time: 2 •socket: /var/run/mysqld/mysqld.sock •sort_buffer_size: 2097144 •sql_big_selects: ON •sql_mode: STRICT_TRANS_TABLES •sql_notes: ON •sql_warnings: OFF •ssl_ca: /etc/mysql/cacert.pem •ssl_capath: •ssl_cert: /etc/mysql/server-cert.pem •ssl_cipher: •ssl_key: /etc/mysql/server-key.pem •storage_engine: MyISAM •sync_binlog: 0 •sync_frm: ON •system_time_zone: EDT •table_cache: 64 •table_lock_wait_timeout: 50 •table_type: MyISAM •thread_cache_size: 8 •thread_stack: 131072 •time_format: %H:%i:%s •time_zone: SYSTEM •timed_mutexes: OFF •tmp_table_size: 33554432

Device	Protocol	Port	Vulnerabilities	Additional Information
				•tmpdir: /tmp •transaction_alloc_block_size: 8192 •transaction_prealloc_size: 4096 •tx_isolation: REPEATABLE-READ •updatable_views_with_limit: YES •version: 5.0.51a-3ubuntu5 •version_comment: (Ubuntu) •version_compile_machine: i486 •version_compile_os: debian-linux-gnu •wait_timeout: 28800

4.8. NFS

The Network File System provides remote file access to shared file systems across a network. NFS provides methods to list and browse directories and to access and alter files. NFS is built on the RPC protocol and is thus independent of machine, operating systems, or even underlying protocol. The main NFS protocol often operates in tandem with other NFS style protocols. The NFS Mount protocol deals with attaching the remote file systems to a point on the local machine's file system, and advertising what file systems are available to be mounted. The NFS Lock manager adds support for file locking to prevent the occurrence of file change conflicts.

4.8.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	tcp	2049	0	•program-number: 100003 •program-version: 4
192.168.56.3	udp	2049	0	•program-number: 100003 •program-version: 4

4.9. NFS lockd

The Network File System provides remote file access to shared file systems across a network. NFS provides methods to list and browse directories and to access and alter files. NFS is built on the RPC protocol and is thus independent of machine, operating systems, or even underlying protocol. This service, NFS Lock manager, adds support for file locking to prevent the occurrence of file change conflicts. Since the NFS protocol is stateless, the NFS Lock Manager takes care of all the stateful aspects of file locking across a network

4.9.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	tcp	44501	0	•program-number: 100021 •program-version: 4
192.168.56.3	udp	58930	0	•program-number: 100021 •program-version: 4

4.10. Postgres

4.10.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	tcp	5432	1	

4.11. Remote Execution

Remote Execution, rexec, is used to execute a command on a remote system.

4.11.1. General Security Issues

Authentication easily spoofed

The Remote Execution protocol does not use userid/password authentication to validate users. Instead it uses trust relationships based on information that is easily spoofed by an attacker. When a client connects to a rexec server, it sends a user name to the server. The server verifies client access by: 1. verifying the client's TCP port is reserved (below 1024) 2. verifying that the specified user name exists 3. verifying the client's IP address is in /etc/hosts.equiv file (or /.rhosts if root was specified as the user name). 4. verifying that logins have not been disabled (eg, /etc/nologin).

4.11.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	tcp	512	1	

4.12. Remote Login

Remote Login, rlogin, is used to create a virtual terminal on the remote system, similar to a Telnet connection. Unlike Telnet connections, rlogin does not require a password from trusted hosts.

4.12.1. General Security Issues

Authentication easily spoofed

The Remote Login protocol does not use userid/password authentication to validate users. Instead it uses trust relationships based on information that is easily spoofed by an attacker. When a client connects to a rlogin server, it sends a user name to the server. The server verifies client access by: 1. verifying the client's TCP port is reserved (below 1024) 2. verifying that the specified user name exists 3. verifying the client's IP address is in /etc/hosts.equiv file (or /.rhosts if root was specified as the user name). 4. verifying that logins have not been disabled (eg, /etc/nologin).

4.12.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	tcp	513	1	

4.13. Remote Shell

Remote Shell, rsh, is used to open a shell on the remote system. Once a shell is established, the client can execute commands on the remote system and receive the program output.

4.13.1. General Security Issues

Authentication easily spoofed

The Remote Shell protocol does not use userid/password authentication to validate users. Instead it uses trust relationships based on information that is easily spoofed by an attacker. When a client connects to a rsh server, it sends a user name to the server. The server verifies client access by: 1. verifying the client's TCP port is reserved (below 1024) 2. verifying that the specified user name exists 3. verifying the client's IP address is in /etc/hosts.equiv file (or /.rhosts if root was specified as the user name). 4. verifying that logins have not been disabled (eg, /etc/nologin).

4.13.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	tcp	514	1	

4.14. SMTP

SMTP, the Simple Mail Transfer Protocol, is the Internet standard way to send e-mail messages between hosts. Clients typically submit outgoing e-mail to their SMTP server, which then forwards the message on through other SMTP servers until it reaches its final destination.

4.14.1. General Security Issues

Installed by default

By default, most UNIX workstations come installed with the sendmail (or equivalent) SMTP server to handle mail for the local host (e.g. the output of some cron jobs is sent to the root account via email). Check your workstations to see if sendmail is running, by telnetting to port 25/tcp. If sendmail is running, you will see something like this: $ telnet mybox 25 Trying 192.168.0.1... Connected to mybox. Escape character is '^]'. 220 mybox. ESMTP Sendmail 8.12.2/8.12.2; Thu, 9 May 2002 03:16:26 -0700 (PDT) If sendmail is running and you don't need it, then disable it via /etc/rc.conf or your operating system's equivalent startup configuration file. If you do need SMTP for the localhost, make sure that the server is only listening on the loopback interface (127.0.0.1) and is not reachable by other hosts. Also be sure to check port 587/tcp, which some versions of sendmail use for outgoing mail submissions.

Promiscuous relay

Perhaps the most common security issue with SMTP servers is servers which act as a "promiscuous relay", or "open relay". This describes servers which accept and relay mail from anywhere to anywhere. This setup allows unauthenticated 3rd parties (spammers) to use your mail server to send their spam to unwitting recipients. Promiscuous relay checks are performed on all discovered SMTP servers. See "smtp-general-openrelay" for more information on this vulnerability and how to fix it.

4.14.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	tcp	25	3	•Postfix •advertise-esmtp: 1 •advertised-esmtp-extension-count: 8 •advertises-esmtp: TRUE •max-message-size: 10240000 •smtp.banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu) •ssl.cert.issuer.dn: EMAILADDRESS=root@ubuntu804-base.localdomain, CN=ubuntu804-base.localdomain, OU=Office for Complication of Otherwise Simple Affairs, O=OCOSA, L=Everywhere, ST=There is no such thing outside

Device	Protocol	Port	Vulnerabilities	Additional Information
				US, C=XX •ssl.cert.key.alg.name: RSA •ssl.cert.key.rsa.modulusBits: 1024 •ssl.cert.not.valid.after: Sat, 17 Apr 2010 00:07:45 EST •ssl.cert.not.valid.before: Thu, 18 Mar 2010 01:07:45 EST •ssl.cert.selfsigned: true •ssl.cert.serial.number: 18084549878917544396 •ssl.cert.sig.alg.name: SHA1withRSA •ssl.cert.subject.dn: EMAILADDRESS=root@ubuntu804-base.localdomain, CN=ubuntu804-base.localdomain, OU=Office for Complication of Otherwise Simple Affairs, O=OCOSA, L=Everywhere, ST=There is no such thing outside US, C=XX •ssl.cert.validsignature: true •supports-8bitmime: TRUE •supports-debug: FALSE •supports-dsn: TRUE •supports-enhancedstatuscodes: TRUE •supports-etrn: TRUE •supports-expand: FALSE •supports-pipelining: TRUE •supports-size: TRUE •supports-starttls: TRUE •supports-turn: FALSE •supports-verify: FALSE •supports-vrfy: TRUE

4.15. SSH

SSH, or Secure SHell, is designed to be a replacement for the aging Telnet protocol. It primarily adds encryption and data integrity to Telnet, but can also provide superior authentication mechanisms such as public key authentication.

4.15.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	tcp	22	2	•OpenSSH 4.7p1 •ssh.banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

Device	Protocol	Port	Vulnerabilities	Additional Information
				•ssh.protocol.version: 2.0 •ssh.rsa.pubkey.fingerprint: 5656240F211DDEA72BAE61B1243 DE8F3

4.16. Telnet

The telnet service provides console access to a machine remotely. All data, including usernames and passwords, is sent in cleartext over TCP. In recent times, most networks have phased out its use in favor for the SSH, or Secure SHell, protocol, which primarily provides strong encryption and superior authentication mechanisms.

4.16.1. General Security Issues

No Support For Encryption

The number one vulnerability that the telnet service faces is its inherent lack of support for encryption. This is an artifact from the time period in which it was invented, 1971. There existed little knowledge of cryptography outside of military environments, and computer technology was not yet advanced enough to handle its real-time use. SSH should be used instead of telnet.

System Architecture Information Leakage

Most telnet servers will broadcast a banner which details the exact system type (ie: hardware and operating system versions) to any connecting client, without requiring authentication. This information is crucial for carrying out serious attacks on the system.

4.16.2. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	tcp	23	1	

4.17. VNC

AT&T VNC is used to provide graphical control of a system. A VNC server can run on a Microsoft Windows, Apple Macintosh or Unix (X Windows) system. By supplying the appropriate password, a VNC server system can be accessed by a VNC client. Full control of the system is provided through VNC, including command execution.

4.17.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	tcp	5900	2	•protocol-version: 3.3 •supported-auth-1: VNC Authentication •supported-auth-count: 1

4.18. XWindows

4.18.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	tcp	6000	0	

4.19. ingreslock (ingres)

4.19.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	tcp	1524	0	

4.20. mountd

4.20.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	udp	33649	1	•program-number: 100005 •program-version: 3
192.168.56.3	tcp	37000	1	•program-number: 100005 •program-version: 3

4.21. portmapper

The Remote Procedure Call portmapper is a service that maps RPC programs to specific ports, and provides that information to client programs. Since most RPC programs do not have a well defined port number, they are dynamically allocated a port number when they are first run. Any client program that wishes to use a particular RPC program first contacts the portmapper to determine the port and protocol of the specified RPC program. The client then uses that information to contact the RPC program directly. In addition some implementations of the portmapper allow tunneling commands to RPC programs through the portmapper.

4.21.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	tcp	111	0	•program-number: 100000 •program-version: 2
192.168.56.3	udp	111	0	•program-number: 100000 •program-version: 2

4.22. status

4.22.1. Discovered Instances of this Service

Device	Protocol	Port	Vulnerabilities	Additional Information
192.168.56.3	udp	48701	0	•program-number: 100024 •program-version: 1
192.168.56.3	tcp	57176	0	•program-number: 100024 •program-version: 1

5. Discovered Users and Groups

5.1. System

5.1.1. 192.168.56.3

Account Name	Type	Additional Information
backup	User	•comment: •user-id: 1068
bin	User	•gid: 2 •loginShell: /bin/sh •password: x •user-id: 2 •userDir: /bin
bind	User	•full-name: •gid: 113 •loginShell: /bin/false •password: x •user-id: 105 •userDir: /var/cache/bind
daemon	User	•gid: 1 •loginShell: /bin/sh •password: x •user-id: 1 •userDir: /usr/sbin
dhcp	User	•comment: •full-name: •user-id: 1202
distccd	User	•comment: •full-name: •user-id: 1222
ftp	User	•comment: •full-name: •user-id: 1214
games	User	•comment: •user-id: 1010
gnats	User	•comment: •full-name: Gnats Bug-Reporting System (admin) •user-id: 1082

Account Name	Type	Additional Information
irc	User	•full-name: ircd •gid: 39 •loginShell: /bin/sh •password: x •user-id: 39 •userDir: /var/run/ircd
klog	User	•full-name: •gid: 104 •loginShell: /bin/false •password: x •user-id: 103 •userDir: /home/klog
libuuid	User	•full-name: •gid: 101 •loginShell: /bin/sh •password: x •user-id: 100 •userDir: /var/lib/libuuid
list	User	•comment: •full-name: Mailing List Manager •user-id: 1076
lp	User	•gid: 7 •loginShell: /bin/sh •password: x •user-id: 7 •userDir: /var/spool/lpd
mail	User	•comment: •user-id: 1016
man	User	•gid: 12 •loginShell: /bin/sh •password: x •user-id: 6 •userDir: /var/cache/man
msfadmin	User	•comment: •full-name: msfadmin,,, •user-id: 3000
mysql	User	•comment: •full-name: MySQL Server,,, •user-id: 1218
news	User	

Account Name	Type	Additional Information
		•gid: 9 •loginShell: /bin/sh •password: x •user-id: 9 •userDir: /var/spool/news
nobody	User	•gid: 65534 •loginShell: /bin/sh •password: x •user-id: 65534 •userDir: /nonexistent
postfix	User	•full-name: •gid: 115 •loginShell: /bin/false •password: x •user-id: 106 •userDir: /var/spool/postfix
postgres	User	•comment: •full-name: PostgreSQL administrator,,, •user-id: 1216
proftpd	User	•full-name: •gid: 65534 •loginShell: /bin/false •password: x •user-id: 113 •userDir: /var/run/proftpd
proxy	User	•gid: 13 •loginShell: /bin/sh •password: x •user-id: 13 •userDir: /bin
root	User	•comment: •user-id: 1000
service	User	•comment: •full-name: ,,, •user-id: 3004
snmp	User	•full-name: •gid: 65534 •loginShell: /bin/false •password: x •user-id: 115

Account Name	Type	Additional Information
		•userDir: /var/lib/snmp
sshd	User	•full-name: •gid: 65534 •loginShell: /usr/sbin/nologin •password: x •user-id: 104 •userDir: /var/run/sshd
statd	User	•full-name: •gid: 65534 •loginShell: /bin/false •password: x •user-id: 114 •userDir: /var/lib/nfs
sync	User	•comment: •user-id: 1008
sys	User	•comment: •user-id: 1006
syslog	User	•full-name: •gid: 103 •loginShell: /bin/false •password: x •user-id: 102 •userDir: /home/syslog
telnetd	User	•comment: •full-name: •user-id: 1224
tomcat55	User	•full-name: •gid: 65534 •loginShell: /bin/false •password: x •user-id: 110 •userDir: /usr/share/tomcat5.5
user	User	•comment: •full-name: just a user,111,, •user-id: 3002
uucp	User	•gid: 10 •loginShell: /bin/sh •password: x •user-id: 10 •userDir: /var/spool/uucp

Account Name	Type	Additional Information
www-data	User	•gid: 33 •loginShell: /bin/sh •password: x •user-id: 33 •userDir: /var/www

5.2. MySQL

5.2.1. 192.168.56.3

Account Name	Type	Additional Information
debian-sys-maint	User	
guest	User	
root	User	

6. Discovered Databases

6.1. MySQL

6.1.1. 192.168.56.3

- dvwa
- information_schema
- metasploit
- mysql
- owasp10
- tikiwiki
- tikiwiki195

7. Discovered Files and Directories

7.1. 192.168.56.3

File/Directory Name	Type	Properties
opt	Directory	•comment: •mount-point: C:\tmp
print$	Directory	•comment: Printer Drivers •mount-point: C:\var\lib\samba\printers
tmp	Directory	•comment: oh noes! •mount-point: C:\tmp

8. Policy Evaluations

No policy evaluations were performed.

9. Spidered Web Sites

No web sites were spidered during the scan.